

# 量子の夢に導かれて

国立研究開発法人 情報通信研究機構

量子ICT協創センター

研究センター長 佐々木 雅英

未来ICT研究所 量子ICT研究室

室長 藤原 幹生

# 概要

1990年代後半、通信総合研究所で産声を上げた量子ICTの研究開発。

これまでの25年間にわたる研究開発を振り返りながら、

社会実装の最前線、

量子セキュリティ拠点整備の現状、

NICTの研究開発戦略を紹介。

今後の展望を皆様とともに議論してまいりたいと思います。

# 量子ICTとは

量子力学で突き詰めた究極の情報通信技術

これまでの歴史をたどりながら当該技術を概観

# 1920年代

## 量子力学の誕生



Heisenberg (1925)

不確定性原理

重ね合わせの原理



Schrödinger (1926)

## 通信の基本概念の誕生

電報や電話の音声をどれだけの速度で伝送できるか？

サンプリング定理  $f_p \leq 2B$

Nyquist (1928)



伝送速度  $R = 2B \log \left( 1 + \frac{A}{\Delta V} \right)$

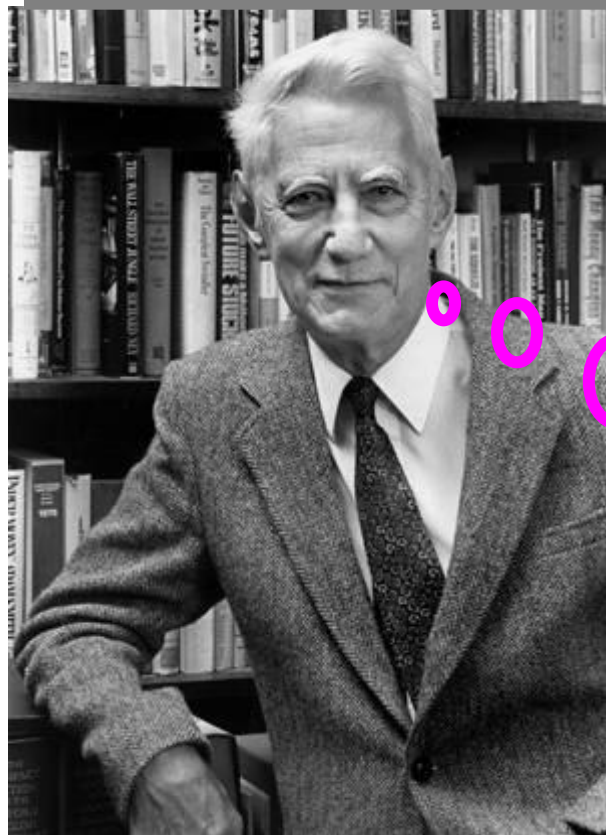
電圧振幅

電圧分解能

Hartley (1928)



# 1948年、通信技術の行く末を決定づける重要な論文

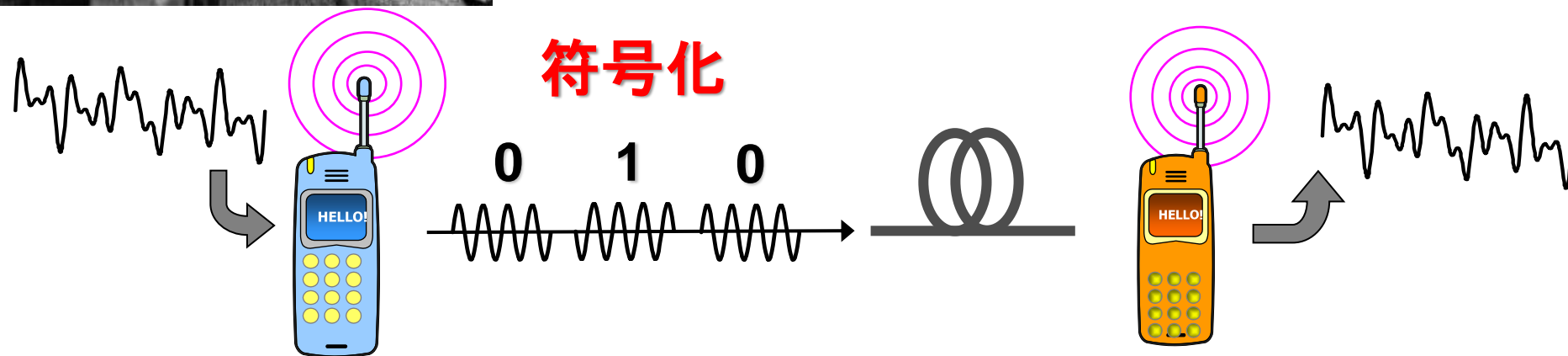


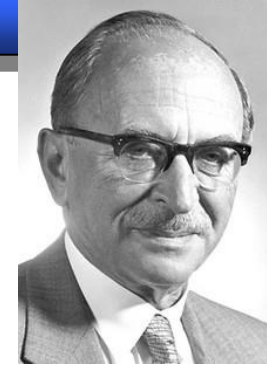
## C. E. Shannonによる通信の基礎理論

ナイキストやハートレーの理論に雑音の効果をきちんと取り入れて体系化

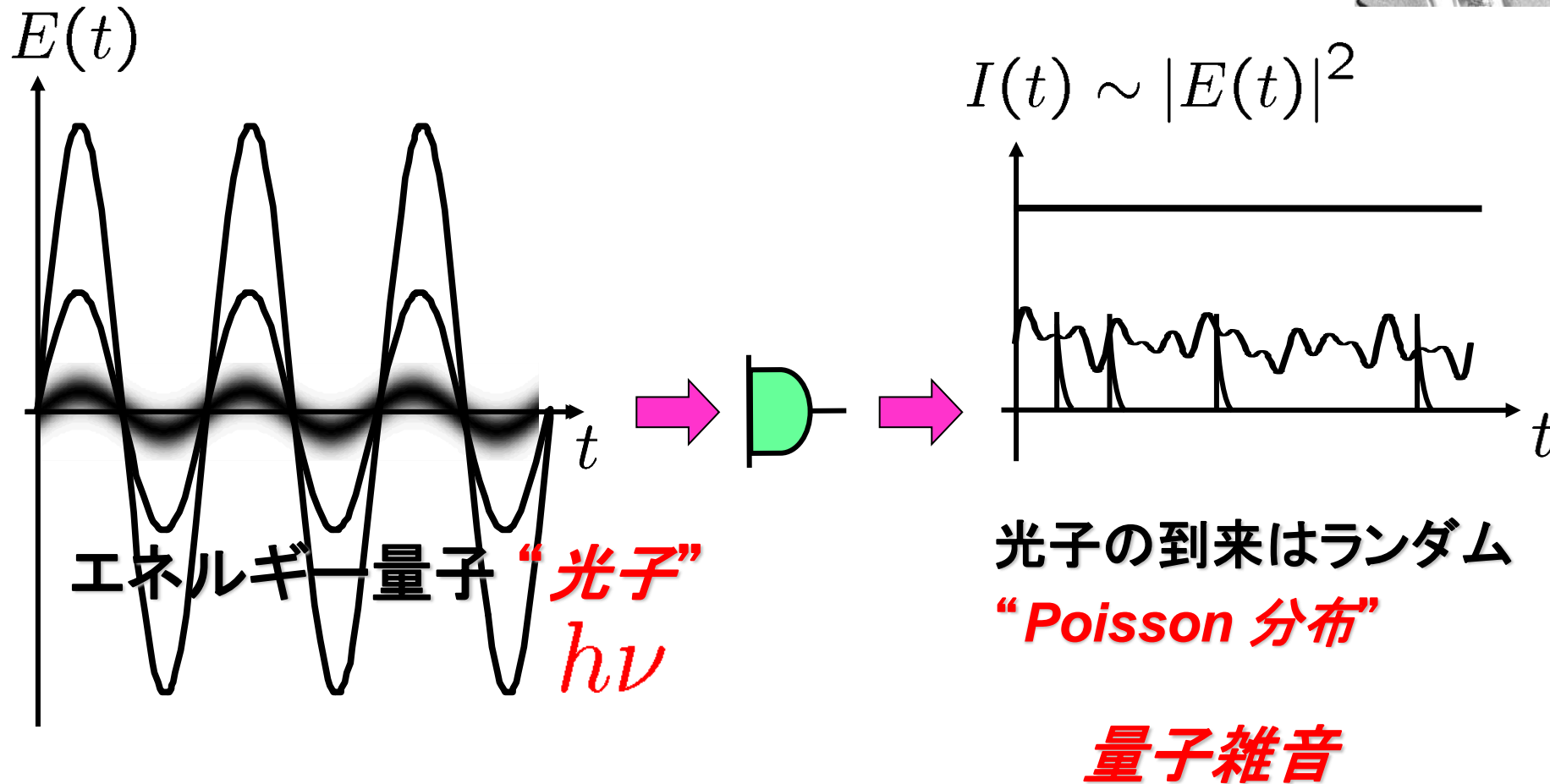
$$C = B \log \left( 1 + \frac{S}{N} \right)$$

雑音があっても符号化を行うことで、誤りのない情報伝送が可能





## 通信における量子効果 D. Gabor 1950



# 1960年代

レーザーの発振に成功 T. H. Maiman 1960

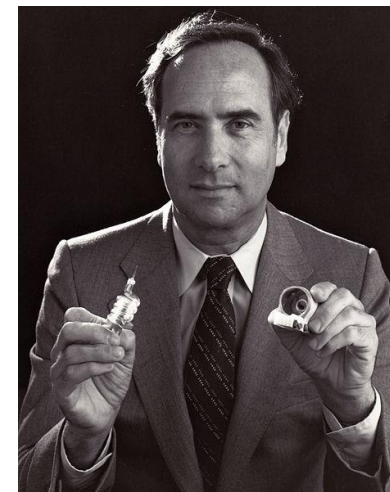
“新時代の幕開け”

レーザー光の  
エネルギー量子  $h\nu \gg k_B T$  室温での  
熱エネルギー  
10000°C      27°C

光子という離散性が顕在化



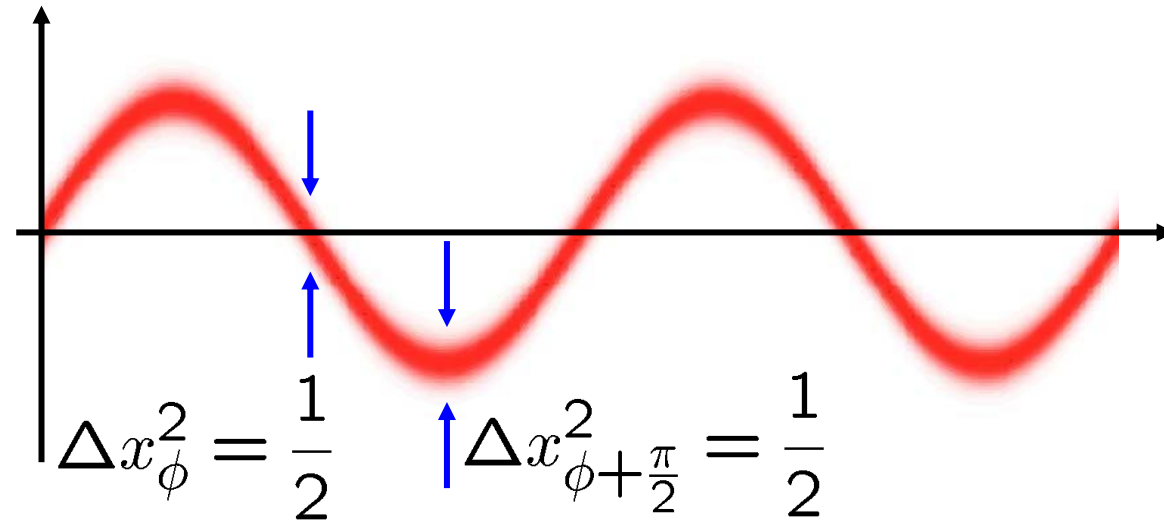
量子雑音を考慮した通信理論が必要



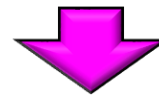
コヒーレント状態という概念を導入し  
レーザーの理論を構築  
R. J. Glauber 1963



ノーベル賞  
(2005)



量子雑音の精密な定式化  $\Delta x_{\phi}^2 \Delta x_{\phi + \frac{\pi}{2}}^2 \geq \frac{1}{4}$



量子光学の誕生



# 量子通信にとっての最初の重要な一歩

## Shannon entropy

$$H(X) = - \sum_x P(x) \log P(x)$$

確率分布



J. P. Gordon (1964)



シャノンの理論を、量子力学  
の言葉を使って置き換える  
“行列力学”

## von Neumann entropy

$$S(\hat{\rho}_x) = -\text{Tr}[\hat{\rho}_x \log \hat{\rho}_x]$$

光の量子状態(行列)



# Gordon予想

Shannonの伝送容量

$$C = \frac{1}{2} \log \left( 1 + \frac{S}{N} \right)$$



J. P. Gordon

伝送容量はもっと上がるだろう…

“上界予想”

$$C \sim S\left(\sum_x p_x \hat{\rho}_x\right) - \sum_x p_x S(\hat{\rho}_x)$$

von Neumann entropy

量子測定の理論が未完成で厳密な証明には至らず

# 1970年代

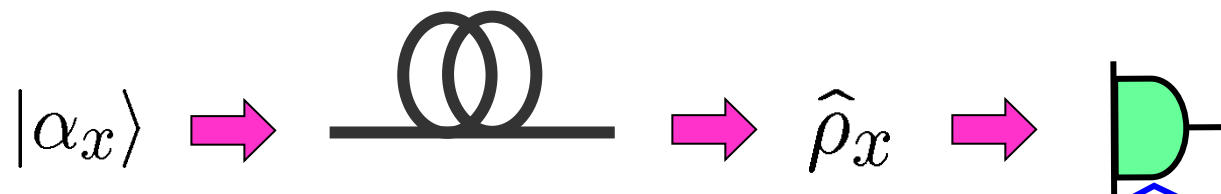
冷戦さなかの米ソで量子測定理論の研究が進展



Helstrom  
Kennedy  
Yuen



Stratonovich  
Belavkin  
Levitin  
Holevo



**Detection operators**  $\sum_y \hat{\Pi}_y = \hat{I}, \quad \hat{\Pi}_y = \hat{\Pi}_y^\dagger > 0$

## Holevo の上界定理 (1973)

量子測定理論を用いGordon予想を厳密に証明

$$C_{\text{Shannon}} \leq \max_{\hat{\Pi}_Y} I(X : Y)$$

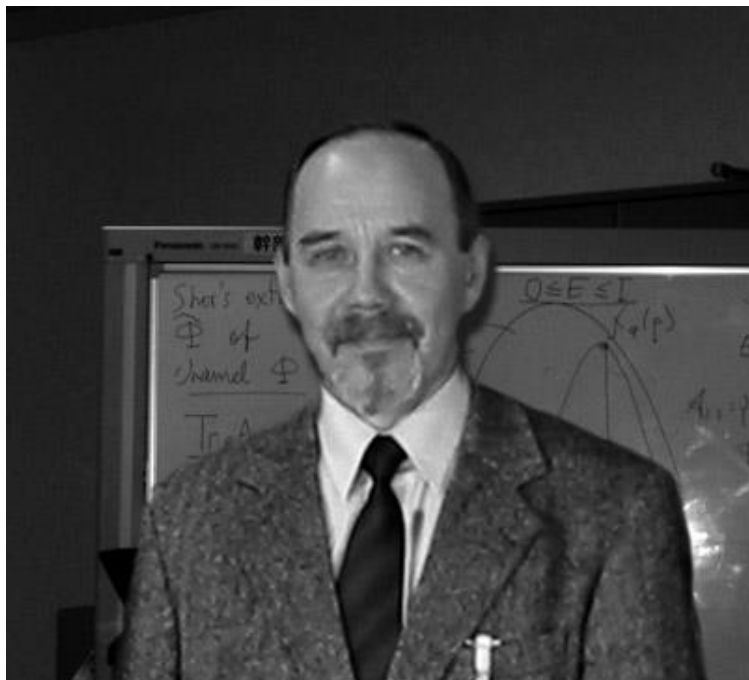
$$\leq S\left(\sum_x p_x \hat{\rho}_x\right) - \sum_x p_x S(\hat{\rho}_x)$$



Holevo上界は真の伝送容量か？

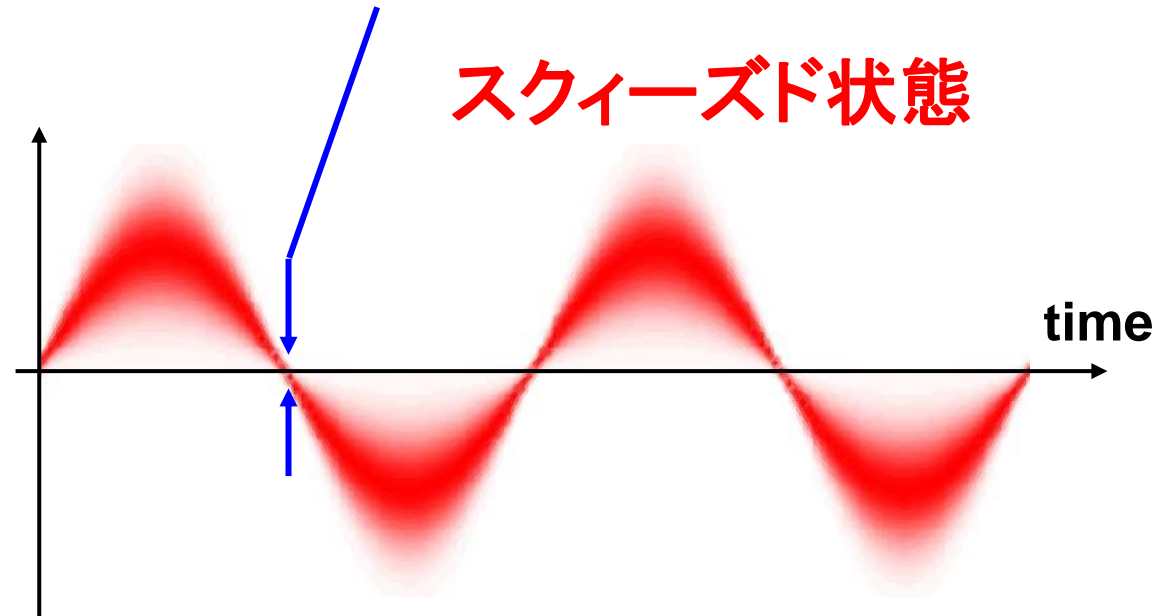


その後、20年以上未解明のままに



# 1980年代、量子光学の進展

量子雑音は絶対に消すことはできないが、  
時間領域を限れば抑圧可能



H. P. Yuen  
(1976)

IBMやATTベル研究所がスクィーズド光生成に成功



超高精度の光計測に新たな道を拓く

# 1980年代

## 量子暗号の誕生



C. H. Bennett

量子力学

1982年  
プエルトリコの  
プールサイド



暗号



G. Brassard

量子鍵配送プロトコル “BB84”  
Quantum Key Distribution (QKD)

## 量子計算の誕生

重ね合わせの原理による超並列処理 (1985)

$$|00\rangle + |01\rangle + |01\rangle + |11\rangle$$



D. Deutsch

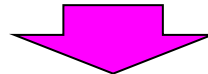
# 1990年代前半

P. W. Shor



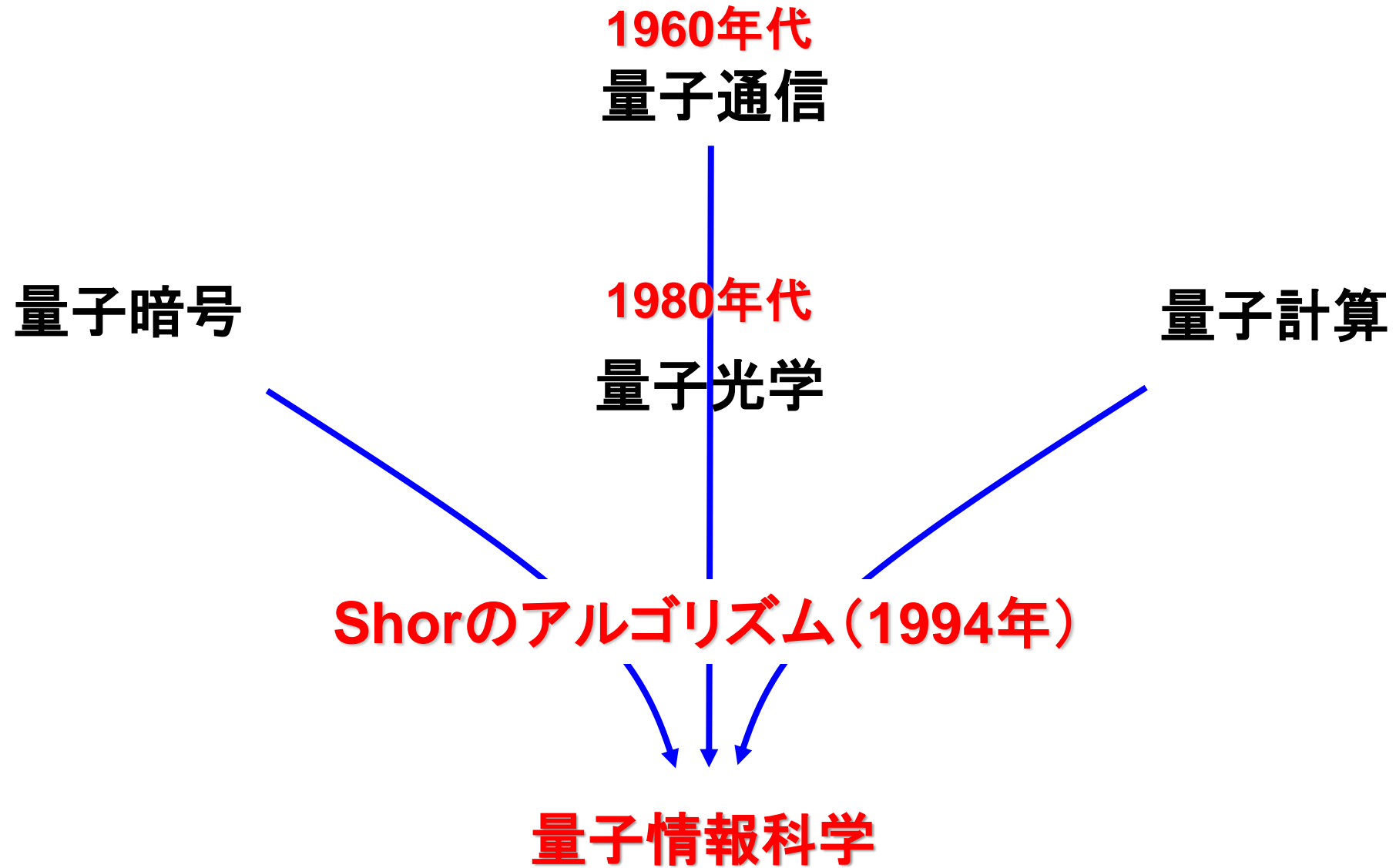
離散対数問題を高速で解く量子アルゴリズム

P. W. Shor,  
"Algorithms for Quantum Computation:  
Discrete Log and Factoring,"  
Proc. of the 35th Annual IEEE Symposium  
on Foundations of Computer Science, 1994.



現代暗号も数分で解読

# 量子情報科学の誕生





# 佐々木雅英 略歴 (1990年代)

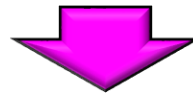
- 1992年 東北大学大学院を卒業、  
日本鋼管株式会社に入社、半導体デバイスの開発に従事
- 1994年 書店で手にした本がきっかけで、量子通信理論の研究を開始
- 1996年 通信総合研究所に入所（光COE特別研究員）、  
光デバイスの研究に従事するかたわら、量子通信理論の研究を継続。

# 1990年代後半

ホレボーの上界定理(1973年)

$$S\left(\sum_x p_x \hat{\rho}_x\right) - \sum_x p_x S(\hat{\rho}_x) \geq C \geq C_1$$

**ホレボー上界**は、実際に達成可能な通信路容量か？



1995年、宇宙論研究者のSchmacherら米英チームが突破口を開く

ホレボー上界が**達成可能な通信路容量である**ことを証明  
(古典雑音が無い場合に限定)

$$C = \max_{\{p_x\}} S\left(\sum_x p_x |\rho_x\rangle\langle\rho_x|\right) \geq C_1$$

Hausladen, et al., Phys. Rev. A54, 1869 (1996).

# 1996年、箱根の国際会議

米英の理論チームとHolevoら旧ソ連の理論家が参加



Holevoが古典雑音まで含む一般的な場合へ証明を拡張

$$C = \max_{\{p_x\}} \left[ S\left(\sum_x p_x \hat{\rho}_x\right) - \sum_x p_x S(\hat{\rho}_x) \right] \geq C_1$$

ホレボ一限界 シャノン限界

- Holevo, IEEE Trans. Inf. Theory IT-44, 269 (1998).
- Schumacher & Westmoreland, Phys. Rev. A 56, 131 (1997).

# シャノン限界を超える通信が可能！⇒ Holevo限界

$$C = \max_{\{p_x\}} \left[ S\left(\sum_x p_x \hat{\rho}_x\right) - \sum_x p_x S(\hat{\rho}_x) \right] > C_1$$

Holevo限界

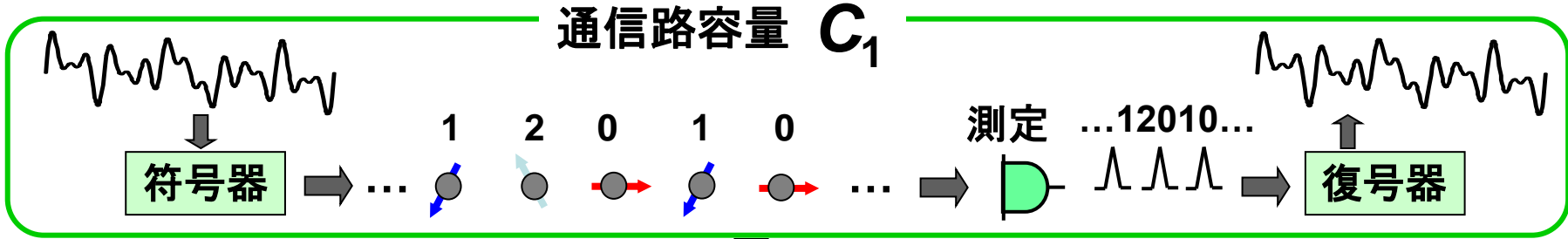
Shannon限界

**具体的にどういう技術を用いれば、新しい通信領域へ踏み出せるか？**

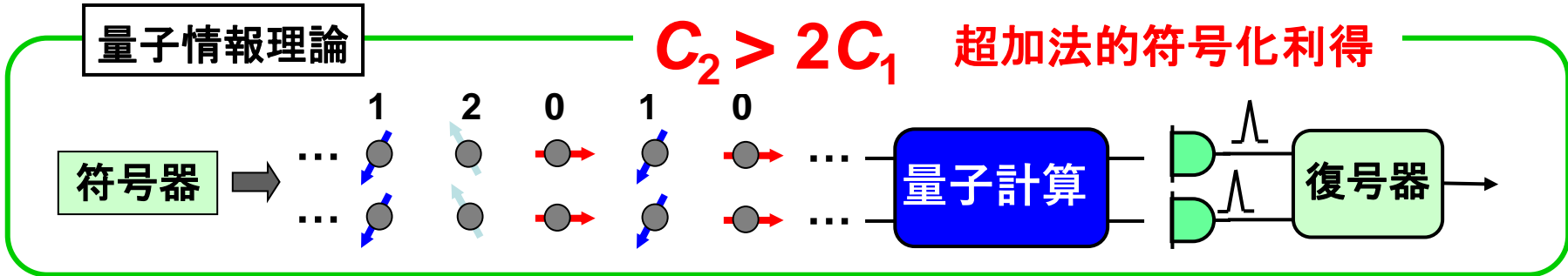
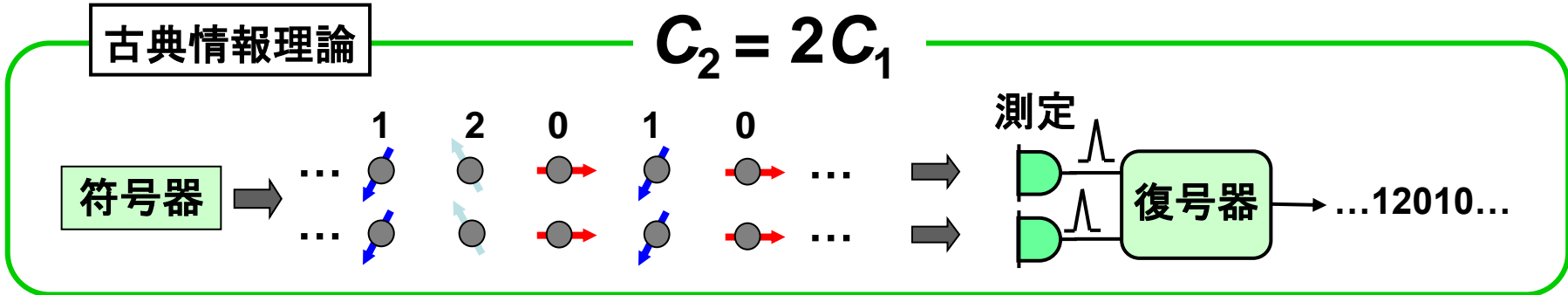
**具体的な符号化の解明に向けた研究**

- Sasaki, et al., Phys. Lett. A236, 1 (1997).
- Sasaki, et al. Phys. Rev. A58, 146 (1998).

# 新しい通信の基本原理は“超加法的符号化利得”



通信帯域を2倍に増やすと ...



**我が国における量子ICT研究開発の立ち上げ**

# 2000年 郵政省

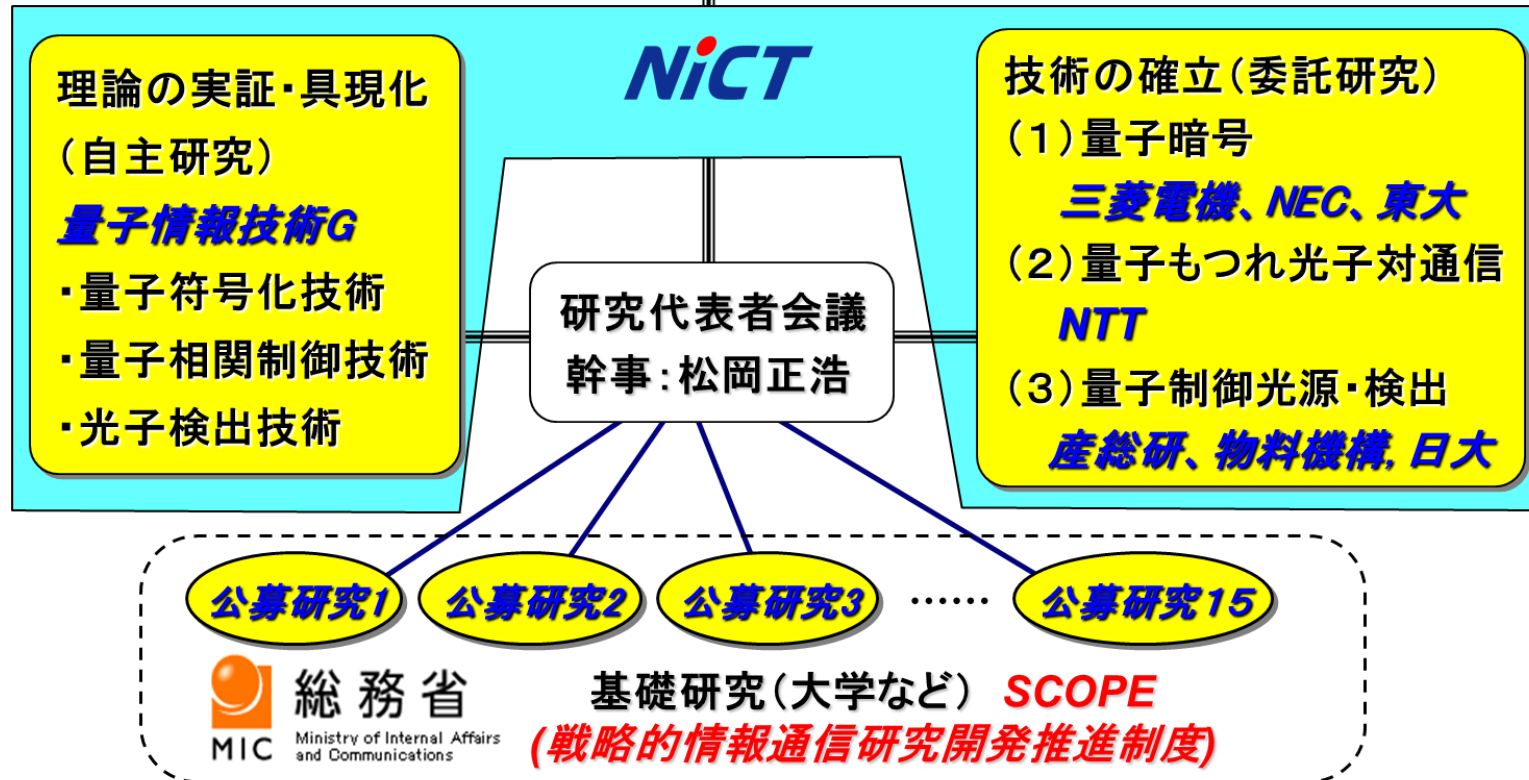
## 「量子力学的効果の情報通信技術への適用とその将来展望に関する研究会」

### 産学官連携による戦略的推進体制

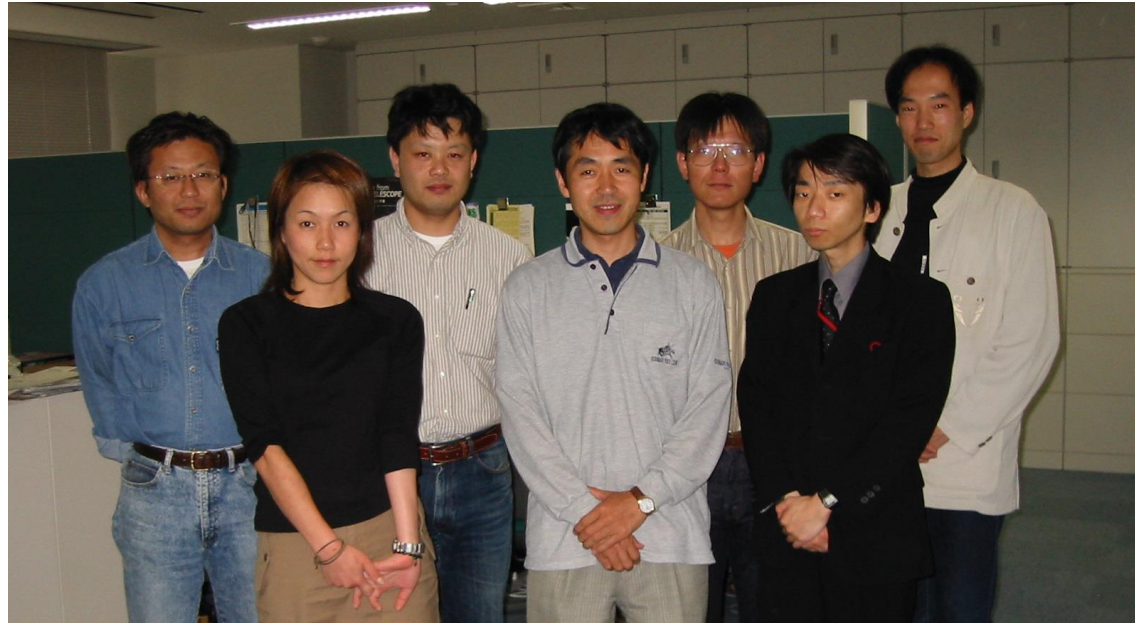
研究推進会議 (議長: 江崎玲於奈)

戦略専門委員会

2001年4月～



# 2001年、通信総合研究所に 量子情報技術研究室が発足





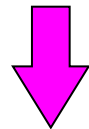
## 2つの柱で研究開発を推進

### 究極の伝送容量

#### 重ね合わせの原理

$$|00\rangle + |01\rangle + |01\rangle + |11\rangle$$

を用いて信号を復号し、  
光子当たりの受信情報量を最大化



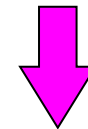
未踏技術の開拓が必要

### 究極の安全性

#### 不確定性原理

$$\Delta x \Delta p \geq h \sim 10^{-34} \text{J}\cdot\text{s}$$

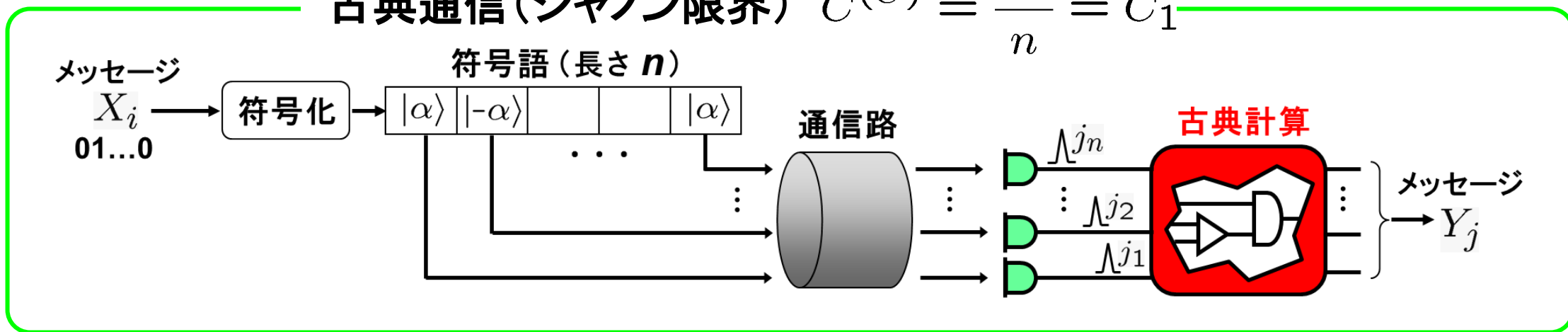
を盗聴者にうまく課して、  
絶対に破られない暗号通信を実現



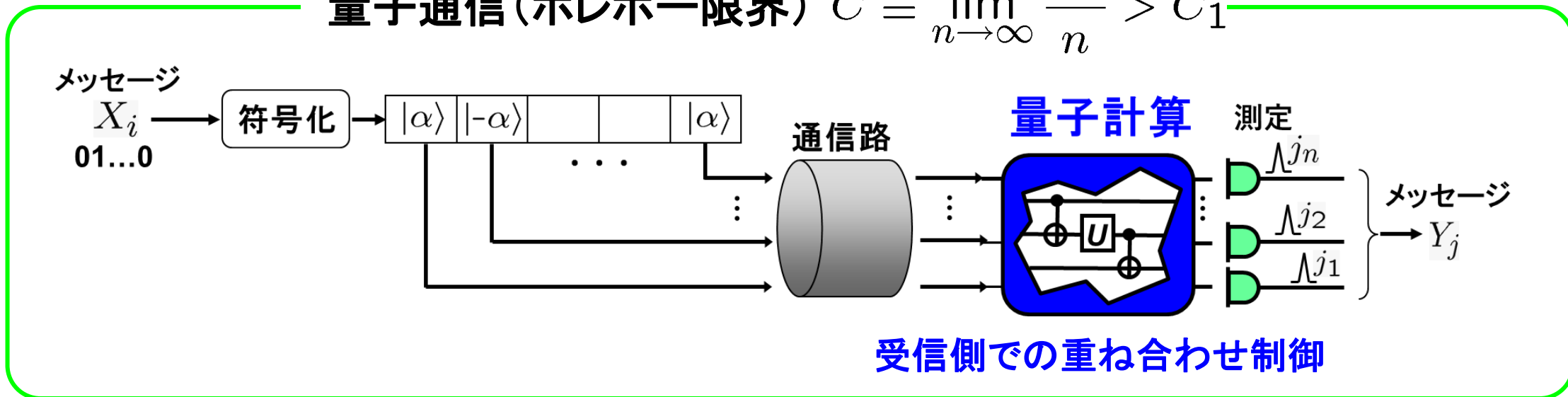
比較的早期に実用化が可能

# 究極の伝送容量

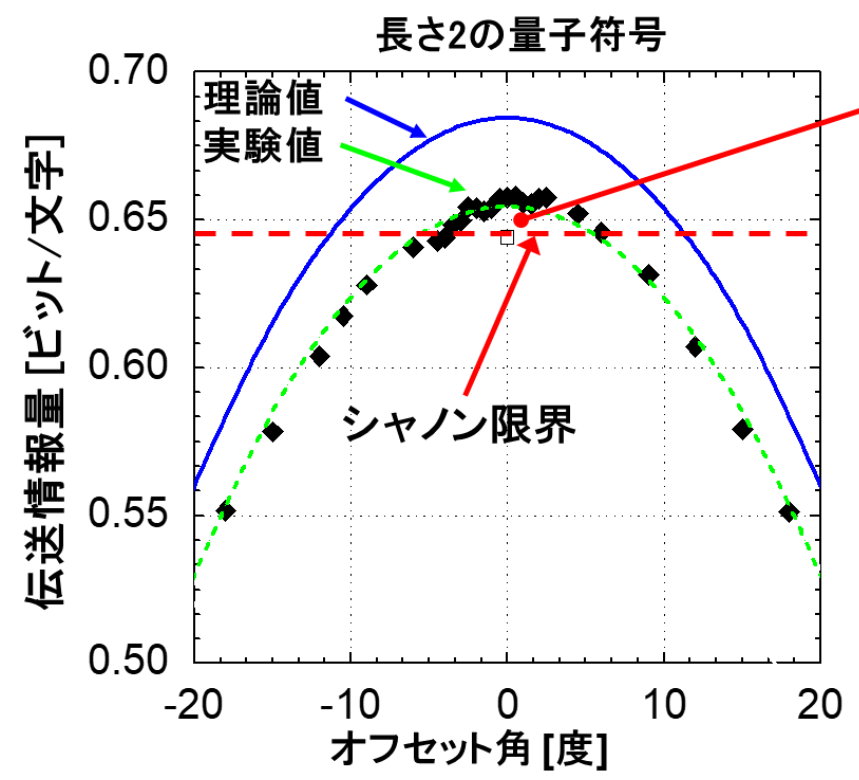
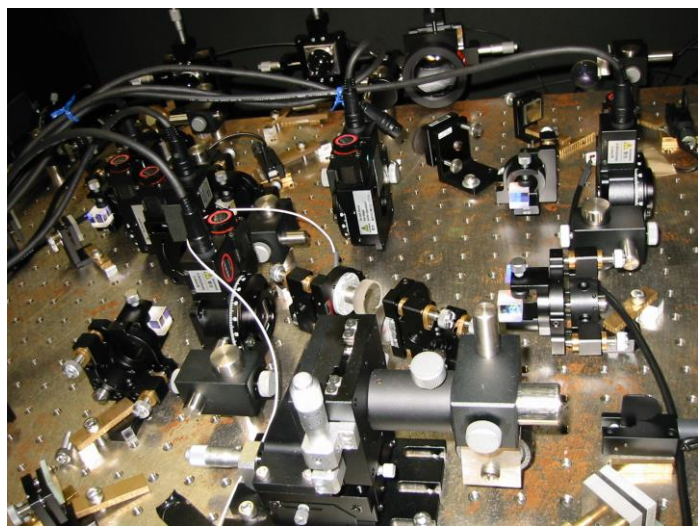
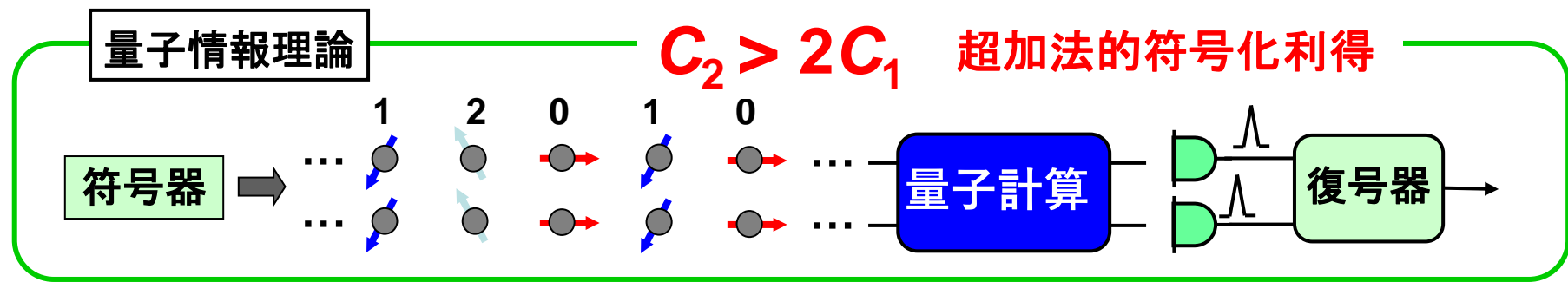
古典通信 (シャノン限界)  $C^{(C)} = \frac{C_n}{n} = C_1$



量子通信 (ホレボー限界)  $C \equiv \lim_{n \rightarrow \infty} \frac{C_n}{n} > C_1$



# 2003年、超加法的符号化利得の実証実験に成功

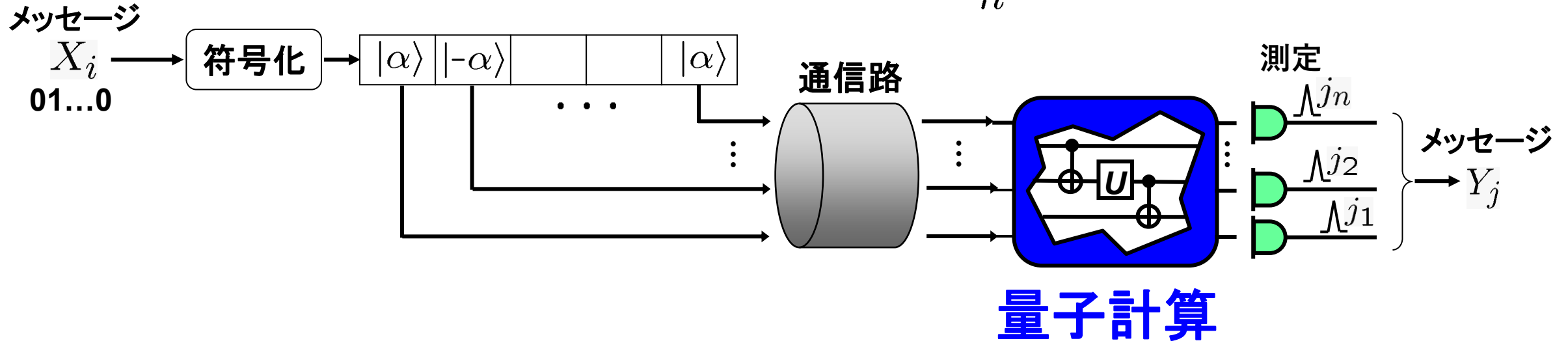


世界で初めて観測された  
超加法的符号化利得

光子の信号帯域を 2 倍  
↓  
2 倍以上の情報量を伝送

# 大規模化に向けた課題

量子通信 : ホレボー限界  $C \equiv \lim_{n \rightarrow \infty} \frac{C_n}{n} > C_1$



受信側における、より大規模な光の重ね合わせ制御技術

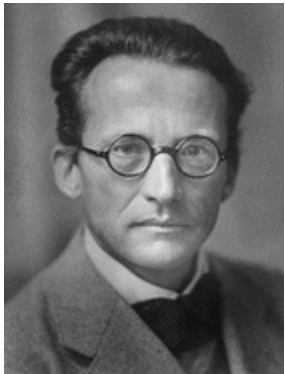
“シュレーディンガーの猫状態”の生成・制御

# 2003年から、『シュレーディンガーの猫状態』の生成に挑戦

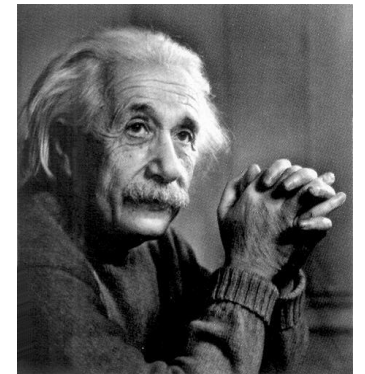
アインシュタインとシュレーディンガーの論争以降、量子光学における積年の夢

## 量子力学のパラドックス(1935年)

量子力学を日常スケールに拡張すると、**猫が生きている状態**  
**と死んでいる状態が共存する重ね合わせ状態**が出現(?)



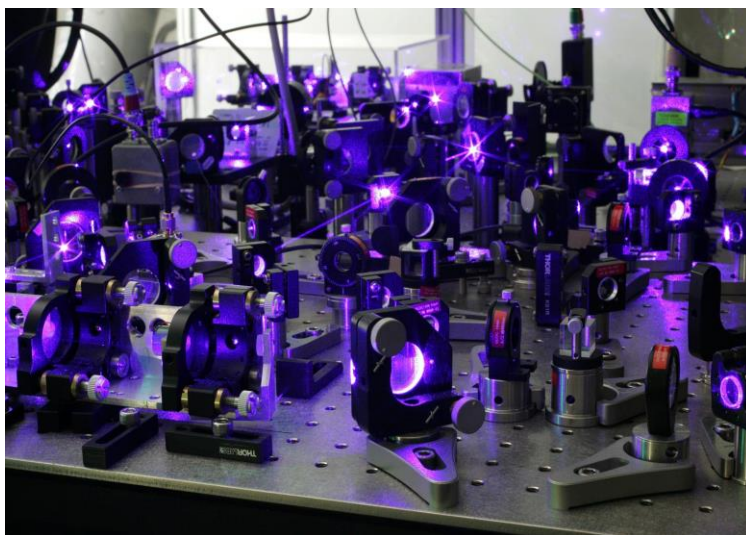
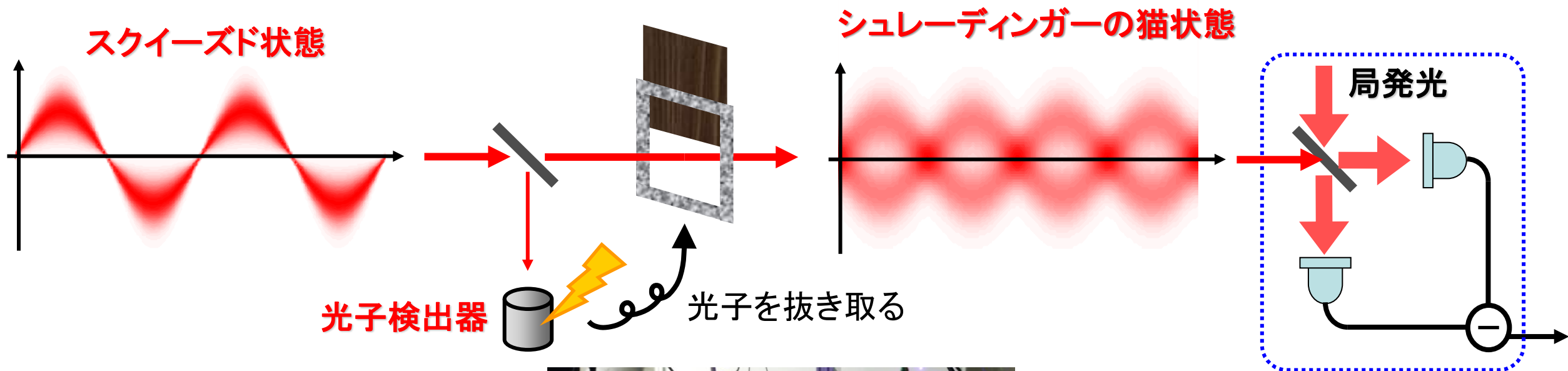
シュレーディンガー



アインシュタイン

# シュレーディンガーの猫状態の生成法

スクイズド状態から光子を抜き取ることで生成

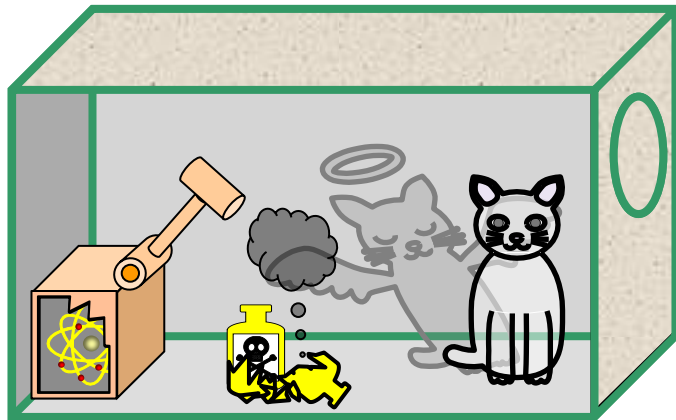


光トモグラフィを用いて  
『Wigner関数』という  
位相空間分布を測定

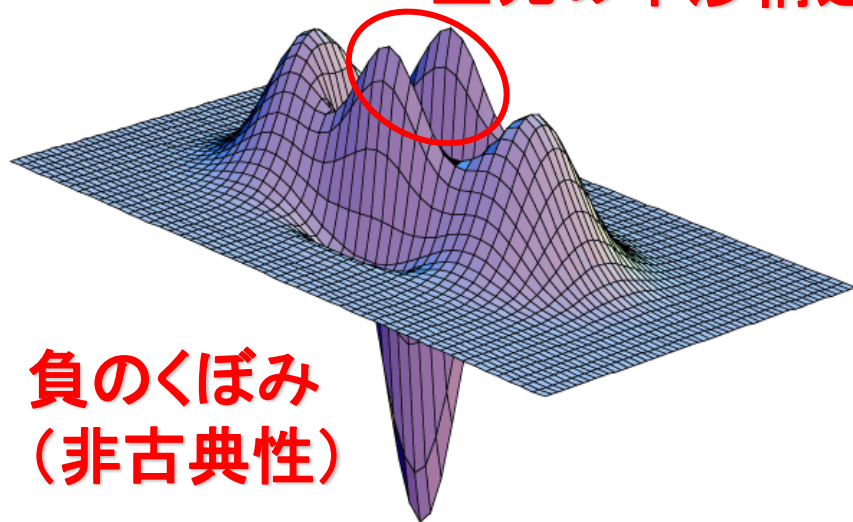
# シュレーディンガーの猫状態 ⇒ 負のWigner関数を観測すること

## 量子の世界

生死が共存する重ね合わせ状態



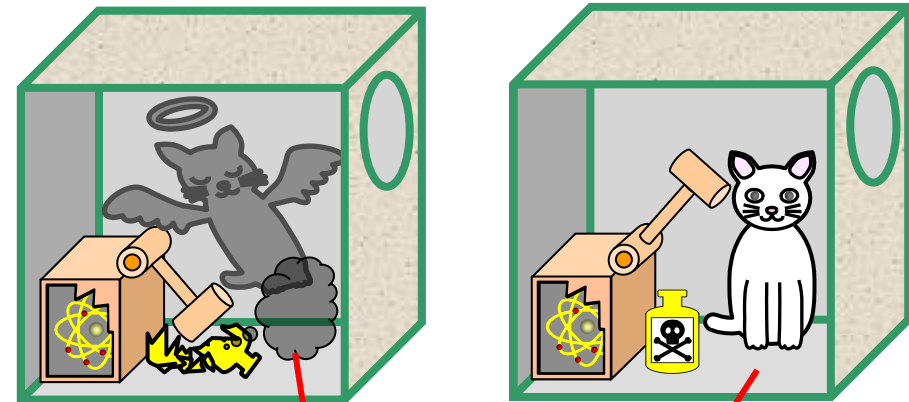
生死の干渉構造



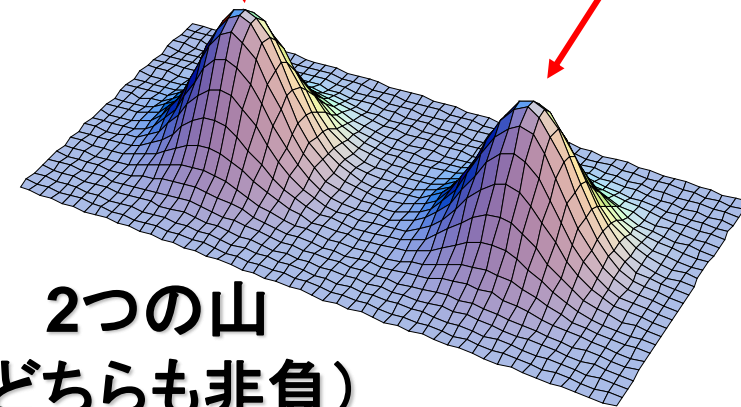
負のくぼみ  
(非古典性)

## 古典の世界

生死が単に分らない状態



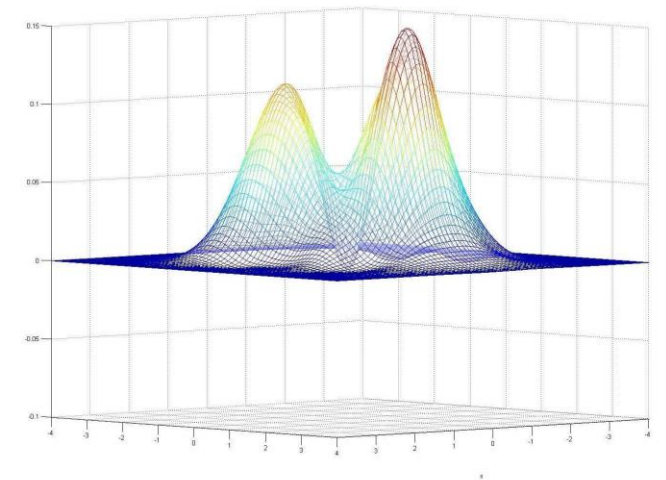
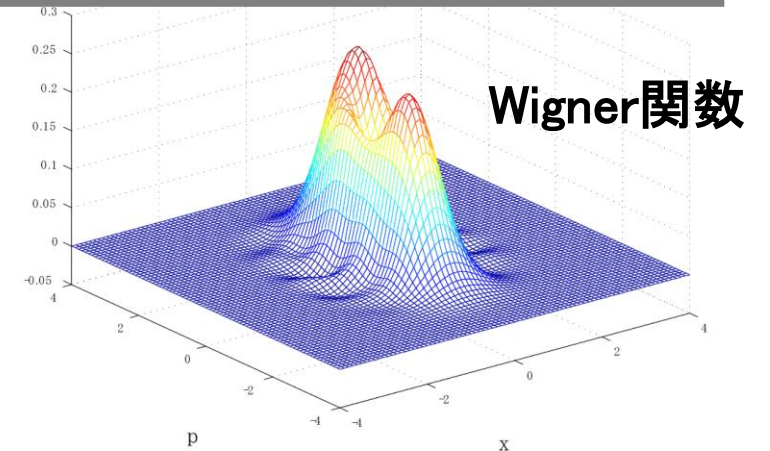
2つの山  
(どちらも非負)



# 立ちどころライバル

実験を繰り返すが、成功しない！  
理論が間違っているのか、実験がまずいのか？

2006年1月、デンマークのニールス・ボーア研究所で、  
シュレーディンガー猫状態の生成に  
成功したらしいとのうわさ。  
2006年3月、プレプリントサイトに実験結果がアップ



一番乗りの夢がスーッと消えてゆく。。。。



# 敗北

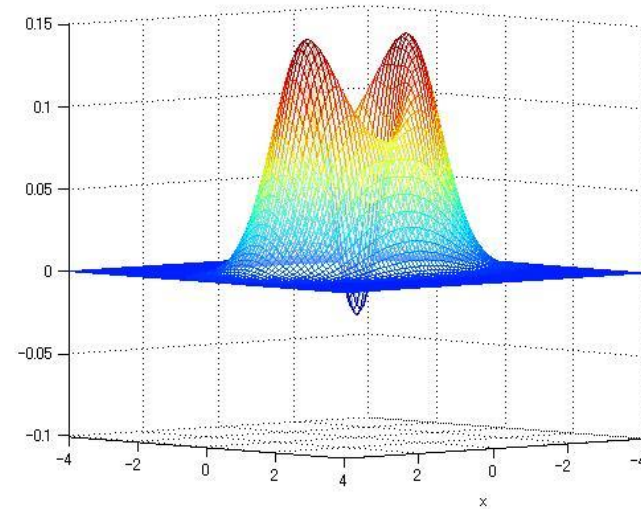
2006年5月、国際会議QCMCの組織委員会

『ニールス・ボーア研究所のE. Polzikを招待しよう』（多くの組織委員）

『それには及ばない。私の招待講演でもっときれいなデータを示す』

（フランスのシャルル・ファブリ研究所、P. Grange）

P. Grangeのチームは、すでに2005年の12月、  
負のWigner関数の観測に成功し、  
サイエンス誌に投稿を済ませていた。



一番乗りの夢は、完全に絶たれ、しばらく茫然自失

# 新たな扉が開く

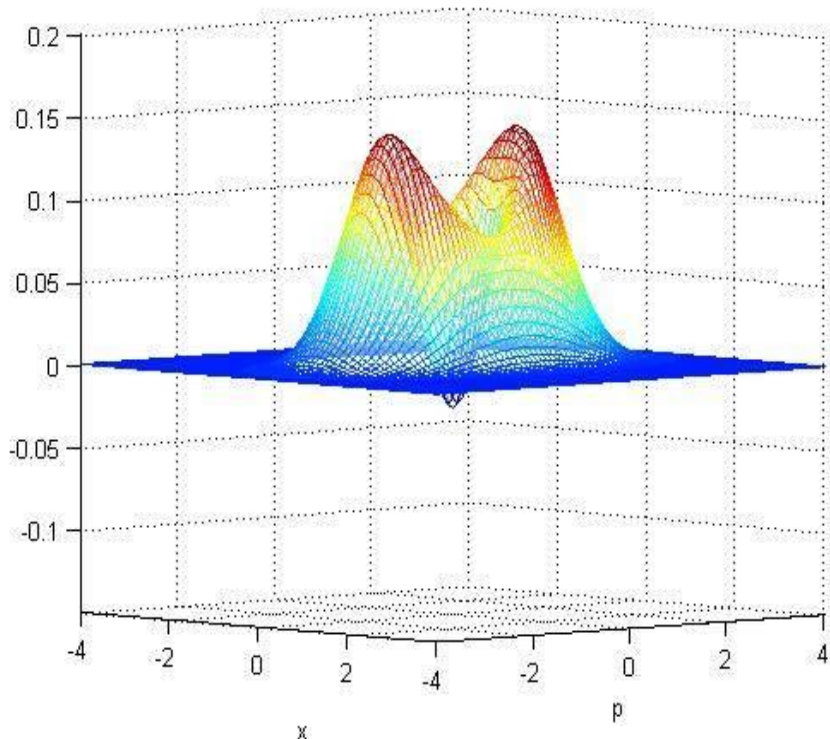
気を取り直し、次の目標に向けて、装置の改良に取り組む。

我々のチームでも、追試に成功、日々、性能が向上。  
しかし、次の目標には、もっと猫状態の純度を上げる必要がある。

2006年8月のある日曜の明け方、4時、佐々木の携帯電話が鳴る。

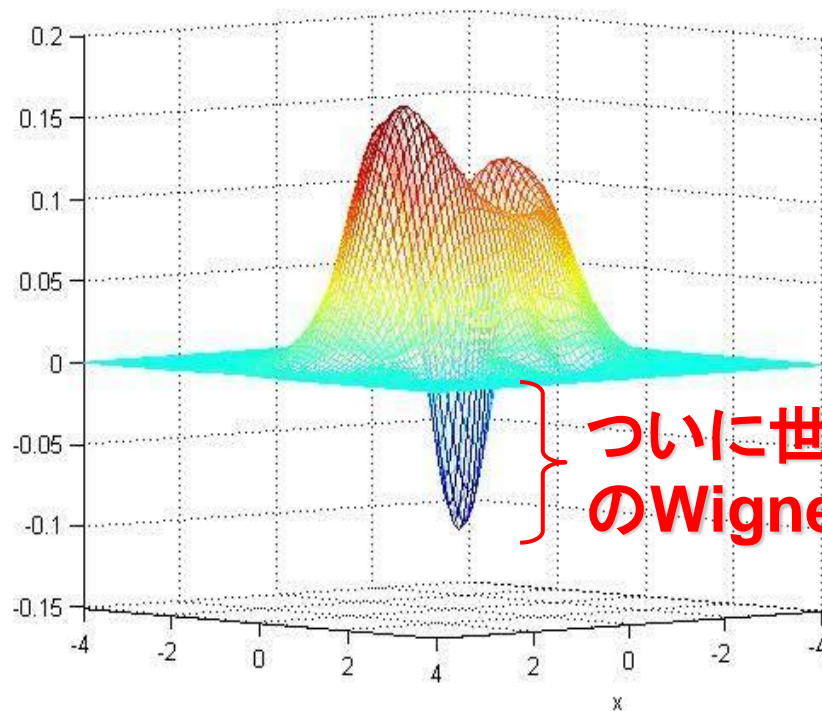
和久井さん(東大の大学院生、NICTの研修生)

**『すごいWigner関数が出ています。見てもらえますか？』**



フランス国立科学研究センター  
(シャルル・ファブリ研究所)

Ourjoumteev, et al.  
Science 312, 83 (2006).  
光源: ポタシウムナイオベート  
( $\text{KNbO}_3$ )

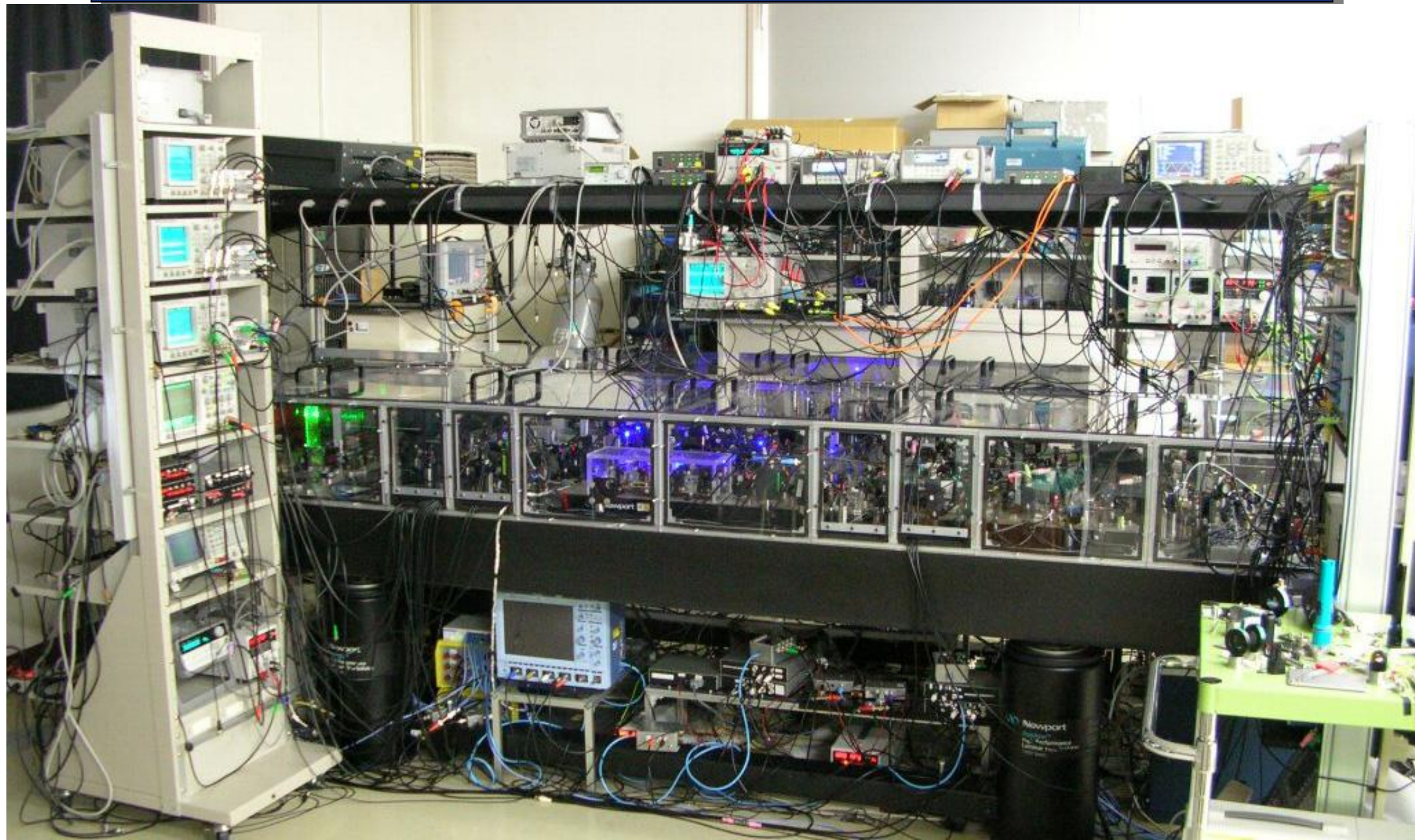


ついに世界最高純度  
のWigner関数を観測

日本、NICT

光学結晶を従来の $\text{KNbO}_3$ から  
新たな結晶 $\text{PP-KTiOPO}_4$ に変えてみた

# 光量子制御の実験装置



# 2007年以降、NICTが先駆的な光量子制御技術を次々と開発

## 猫状態の高純度化、高振幅化に成功

Wakui, et al., Opt. Express 15, 3568 (2007).

Takahashi, et al., Phys. Rev. Lett. 101, 233605 (2008).

## 量子もつれ状態の蒸留に世界で初めて成功

Takahashi, et al. Nature Photonics 4, 178 (2010).

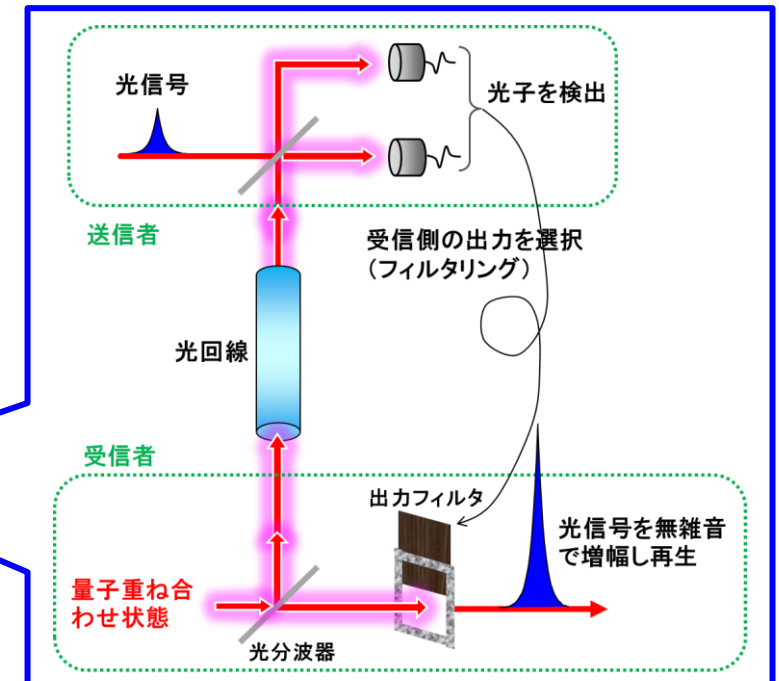
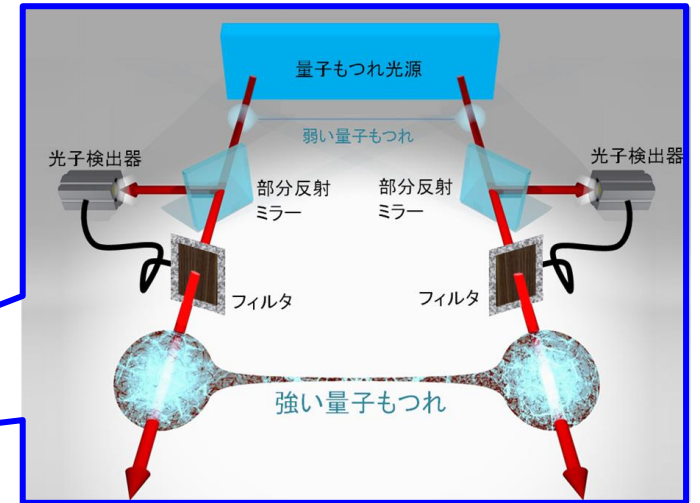
## 猫状態の重ね合わせの自在な制御に成功

Neergaard-Nielsen, et al., Phys. Rev. Lett. 105, 053602 (2010).

Optics and Photonics News誌のOptics in 2010に選出。

## 量子増幅転送に世界で初めて成功

Neergaard-Nielsen, et al., Nature Photonics 7, 439 (2013).



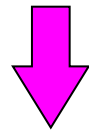
# 量子情報通信

## 究極の伝送容量

### 重ね合わせの原理

$$|00\rangle + |01\rangle + |01\rangle + |11\rangle$$

を用いて信号を復号し、  
光子当たりの受信情報量を最大化



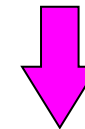
未踏技術の開拓が必要

## 究極の安全性

### 不確定性原理

$$\Delta x \Delta p \geq h \sim 10^{-34} \text{J}\cdot\text{s}$$

を盗聴者にうまく課して、  
絶対に破られない暗号通信を実現



比較的早期に実用化が可能

# 量子暗号

量子力学の法則に基づき、  
どんな計算機でも解読できない暗号通信を実現

2000年代後半からフィールド実験の時代へ

# 2007年、量子暗号の高速化とフィールド実験

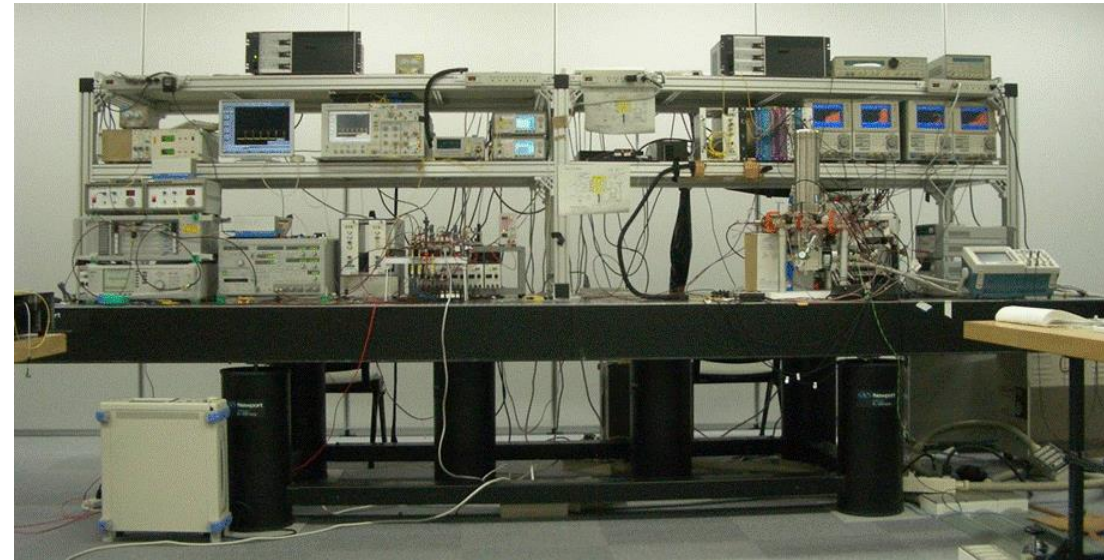
- ・GHzクロックでの高速量子暗号技術を開発
- ・けいはんな地区のネットワーク JGNII 上で97kmのフィールド伝送試験



NEC

NICT

NIST  
National Institute of  
Standards and Technology

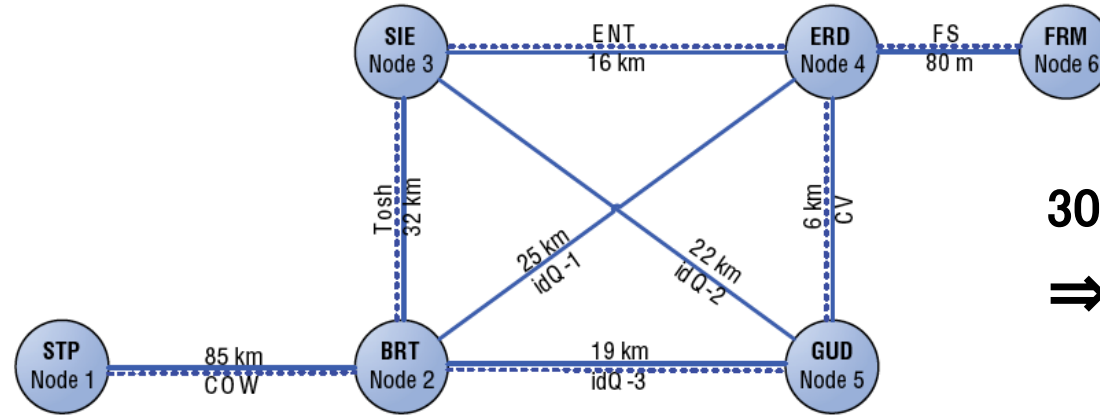


装置はまだ大型のブレッドボードモデル



# 2008年、欧州連合プロジェクトSECOQC

2008年10月、ウィーン市内に都市圏量子暗号ネットワークを構築し、国際会議でデモ



30km圏で鍵生成速度1kbps  
⇒音声の暗号化



SECOQCデモ



SECOQCの各国チームリーダー

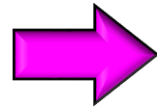


佐々木も招待され

Tokyo QKD Network構想を紹介

# 2010年、Tokyo QKD Networkを構築、運用開始

鍵生成速度を従来比100倍に改善

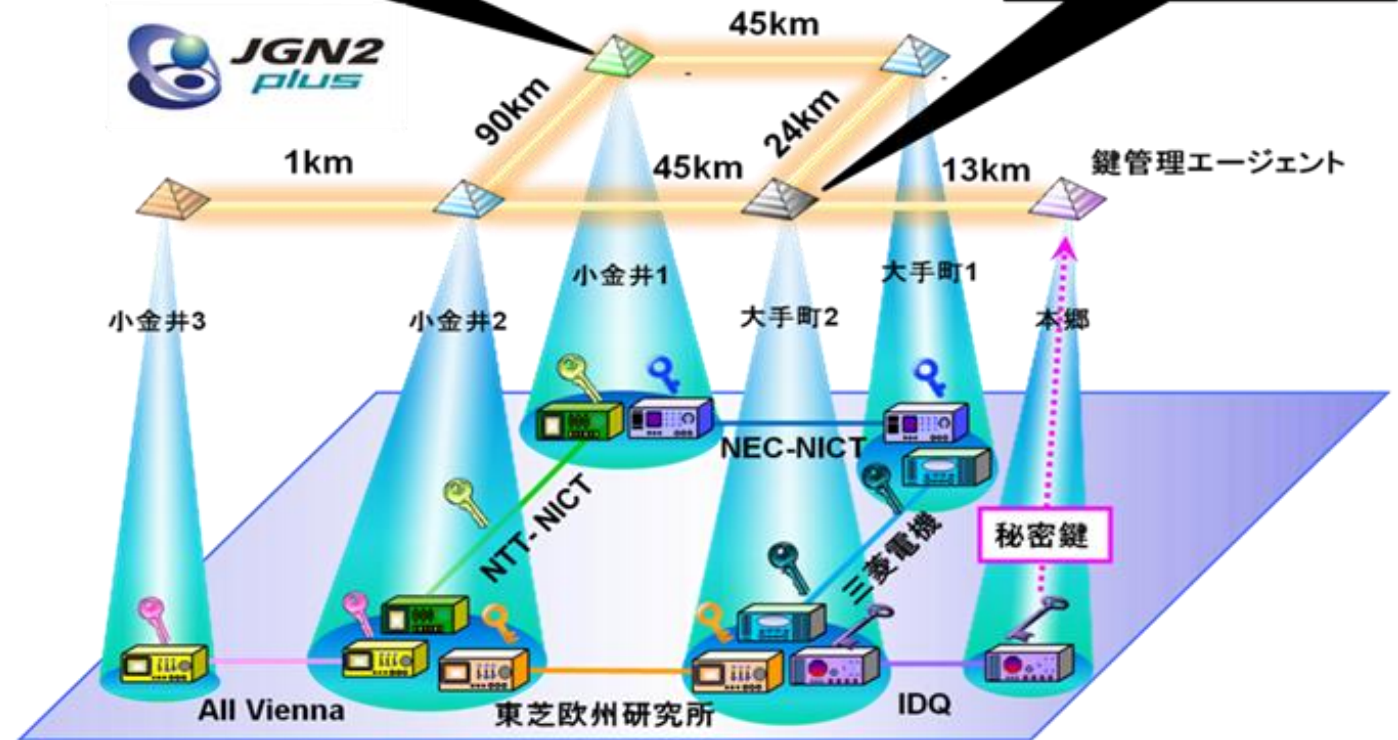


動画の完全秘匿伝送を世界で初めて実現

日本チーム  
NICT  
NEC  
三菱電機  
NTT



世界初



量子暗号・量子通信国際会議(UQCC2010)  
2010年10月18日、ANAインターコンチネンタルホテル東京

Sasaki, et al., Opt. Express (2011).

# 2000年代後半

Secure key rate [bps]

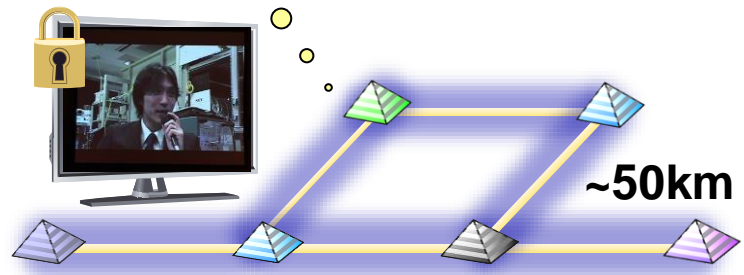
1M

100k

1k

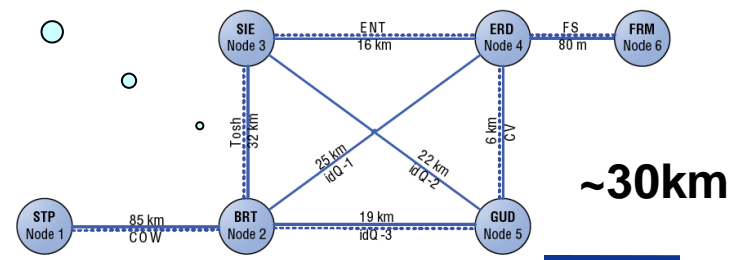
## 動画の量子暗号化

速度を従来比  
100倍に改善



Tokyo QKD Network 

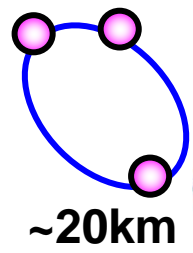
## 音声の量子暗号化



~30km



ベンチャー企業



~20km



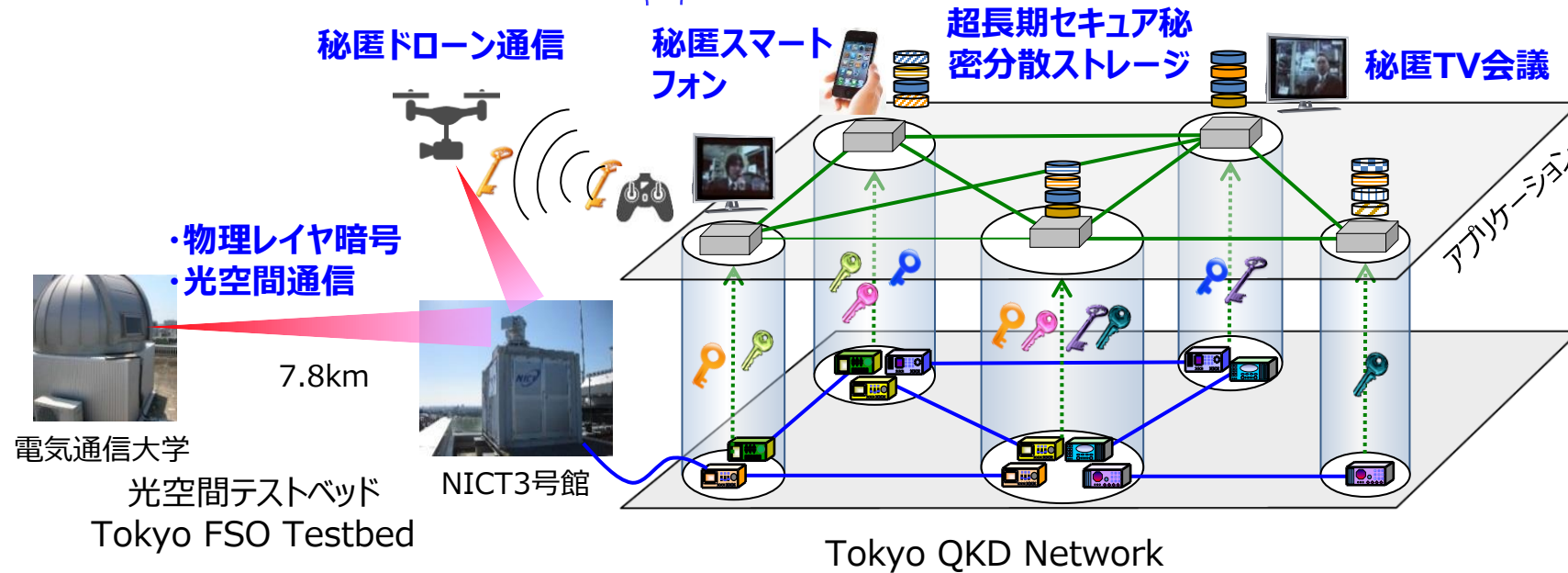
2000

2005

2010

# 2013年、 光空間テストベッドを構築

# 2015年、 新たなQKDアプリケーションを公開デモ

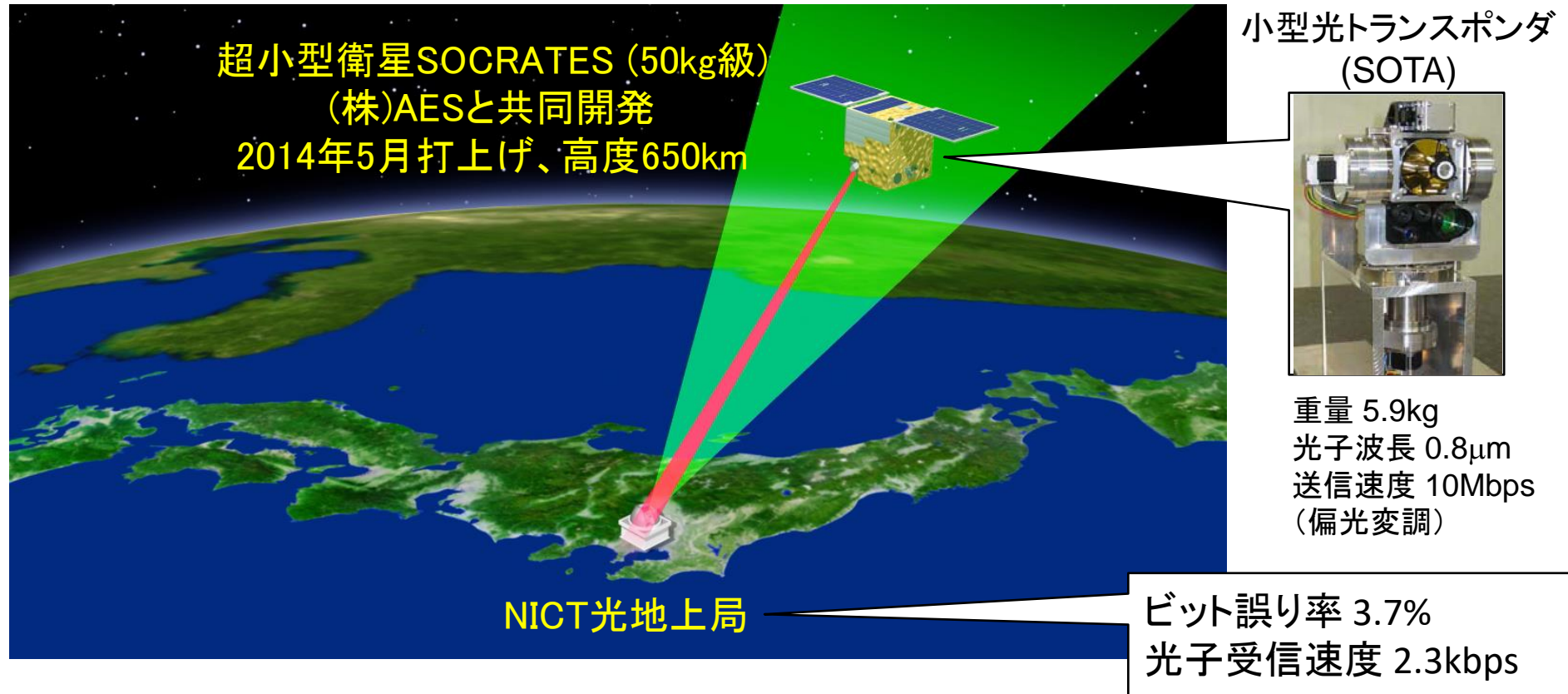


## 量子暗号・量子通信国際会議 UQCC2015 @東京



Bennett、Brassard  
による電子カルテアプリ  
のデモ寸劇

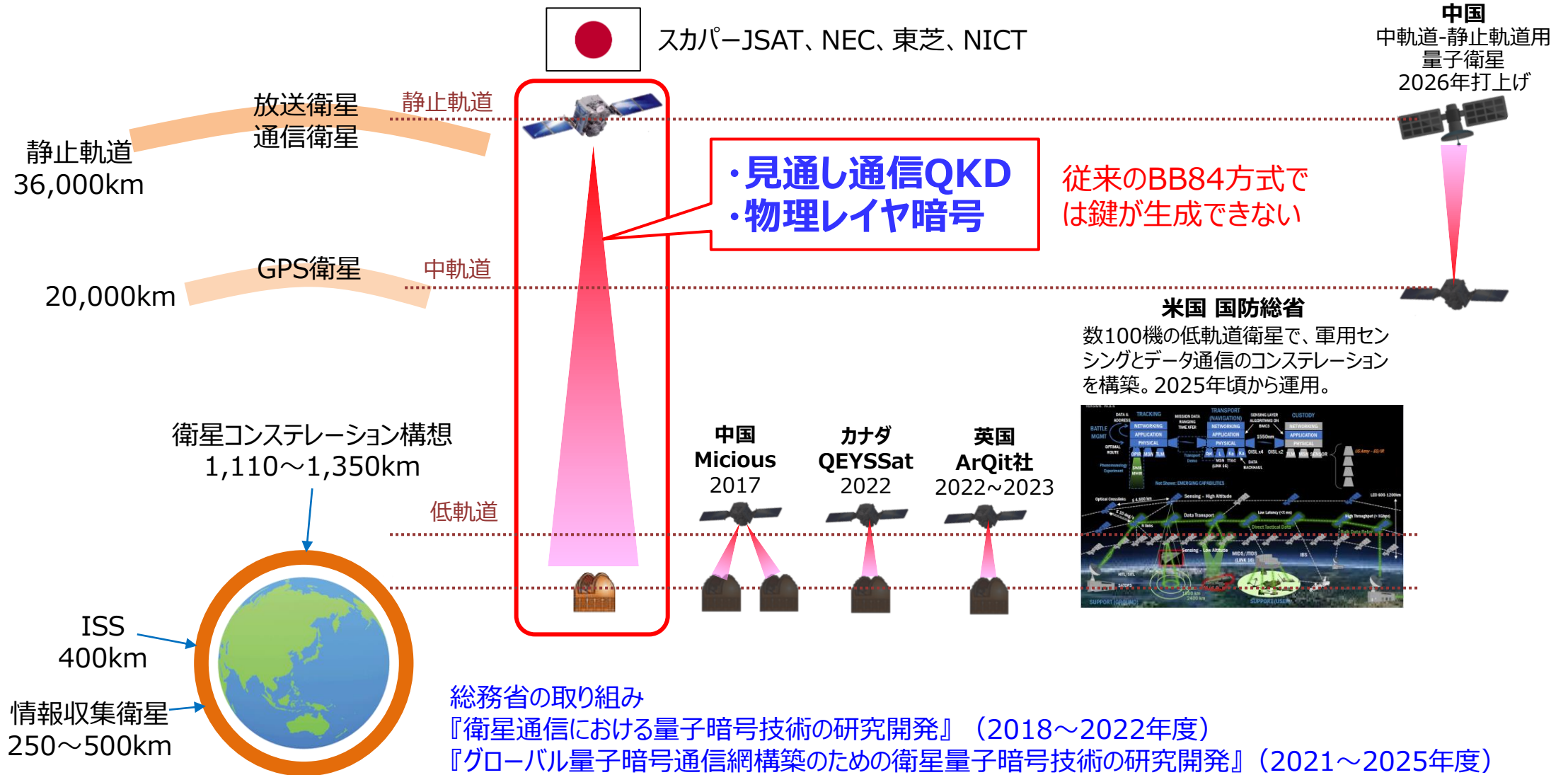
# 2017年、超小型衛星による量子通信の実証実験



- ✓ 光通信分野では世界最小となる50kgの超小型衛星で実現 (中国の量子通信衛星600kgに比べ10分の一)
- ✓ 衛星・地上局間で光子一個一個を制御しながら情報をやりとり

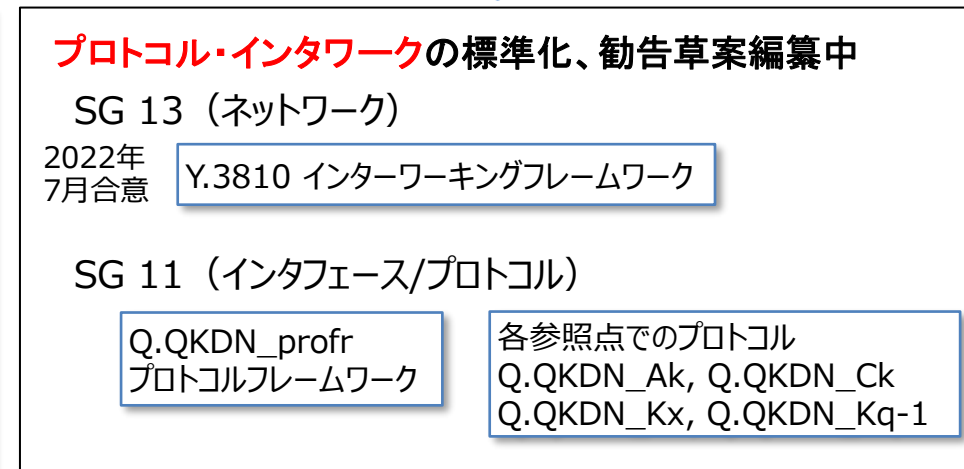
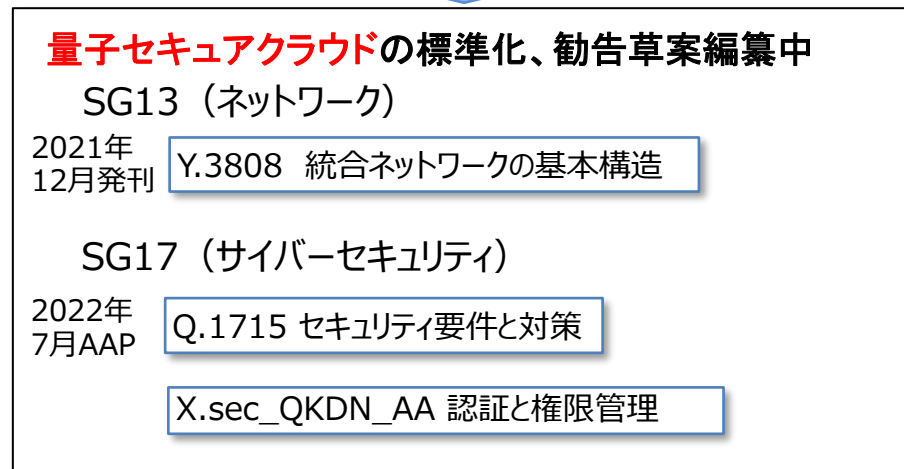
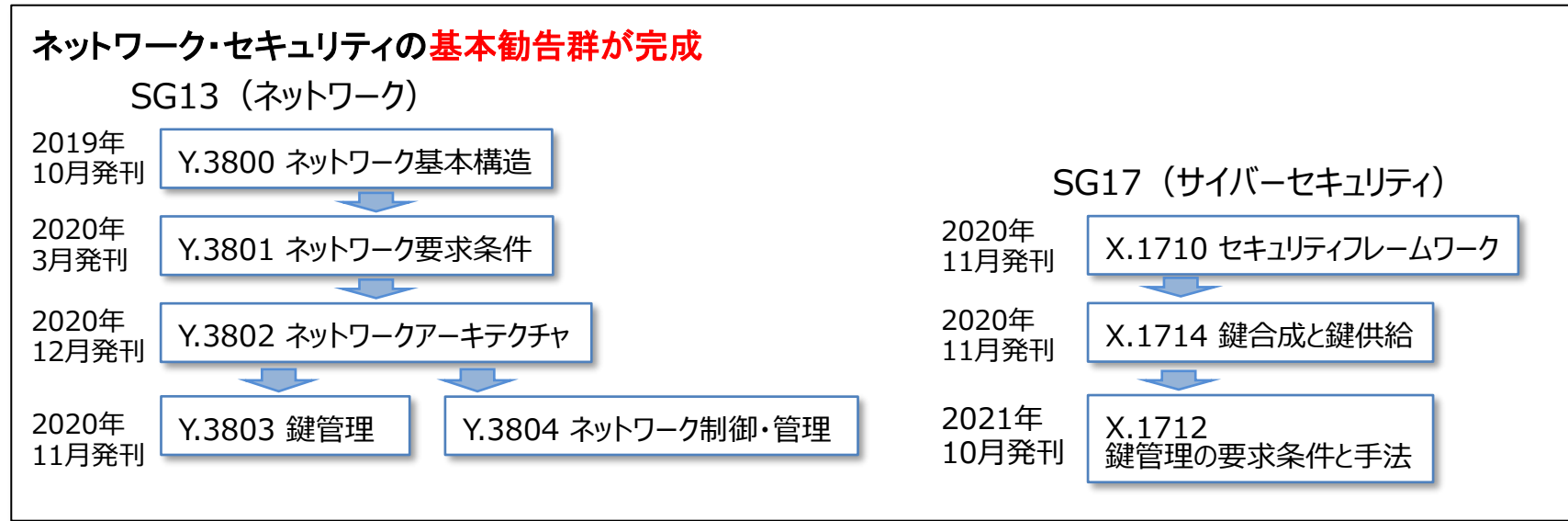
# グローバルネットワーク化に向けて

## 地上局から静止軌道までカバーできる革新的な衛星量子暗号技術を開発



# 2020年、日本の技術を骨子とする基本勧告体系を整備

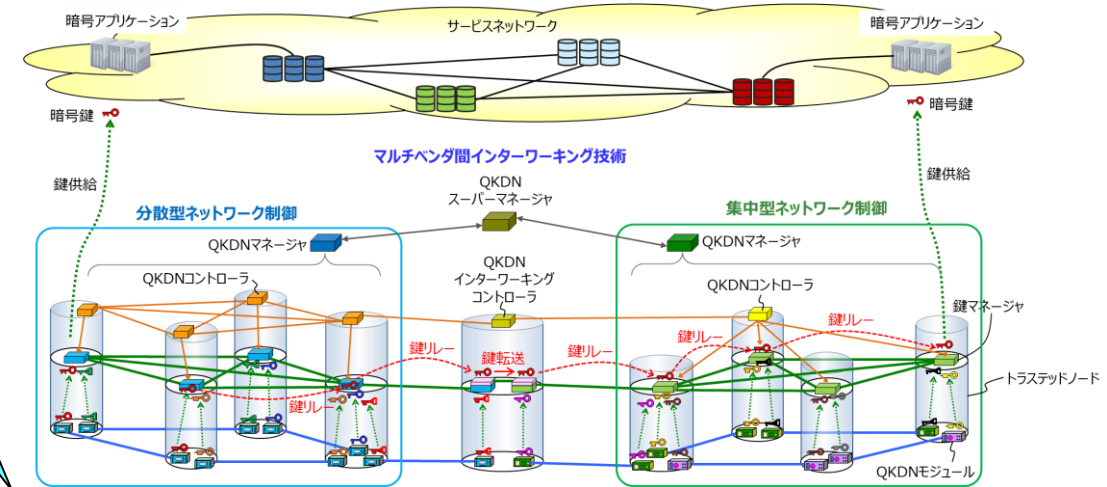
2018年からITU-T等で国際標準化を主導、日本の技術が世界標準に



# ネットワークアーキテクチャの進展

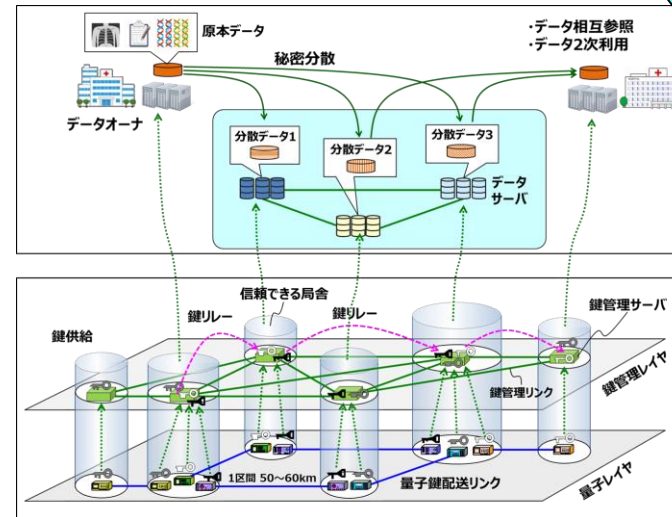
ITU-T勧告草案 Y.QKDN\_iwfr  
マルチベンダインタワーキングの基本構造

## ↑ 広域量子暗号通信網



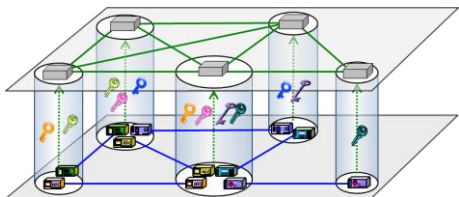
ITU-T勧告 Y.3808  
統合ネットワークの基本構造

## ↑ 量子セキュアクラウド



ITU-T勧告 Y.3800  
QKDネットワークの基本構造





## ↑ Tokyo QKD Network





# 2020年10月、東芝が量子暗号の事業化を発表

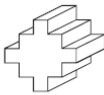
世界最高性能の量子暗号装置。海外製より**10倍高速**、**2倍長距離伝送可能**

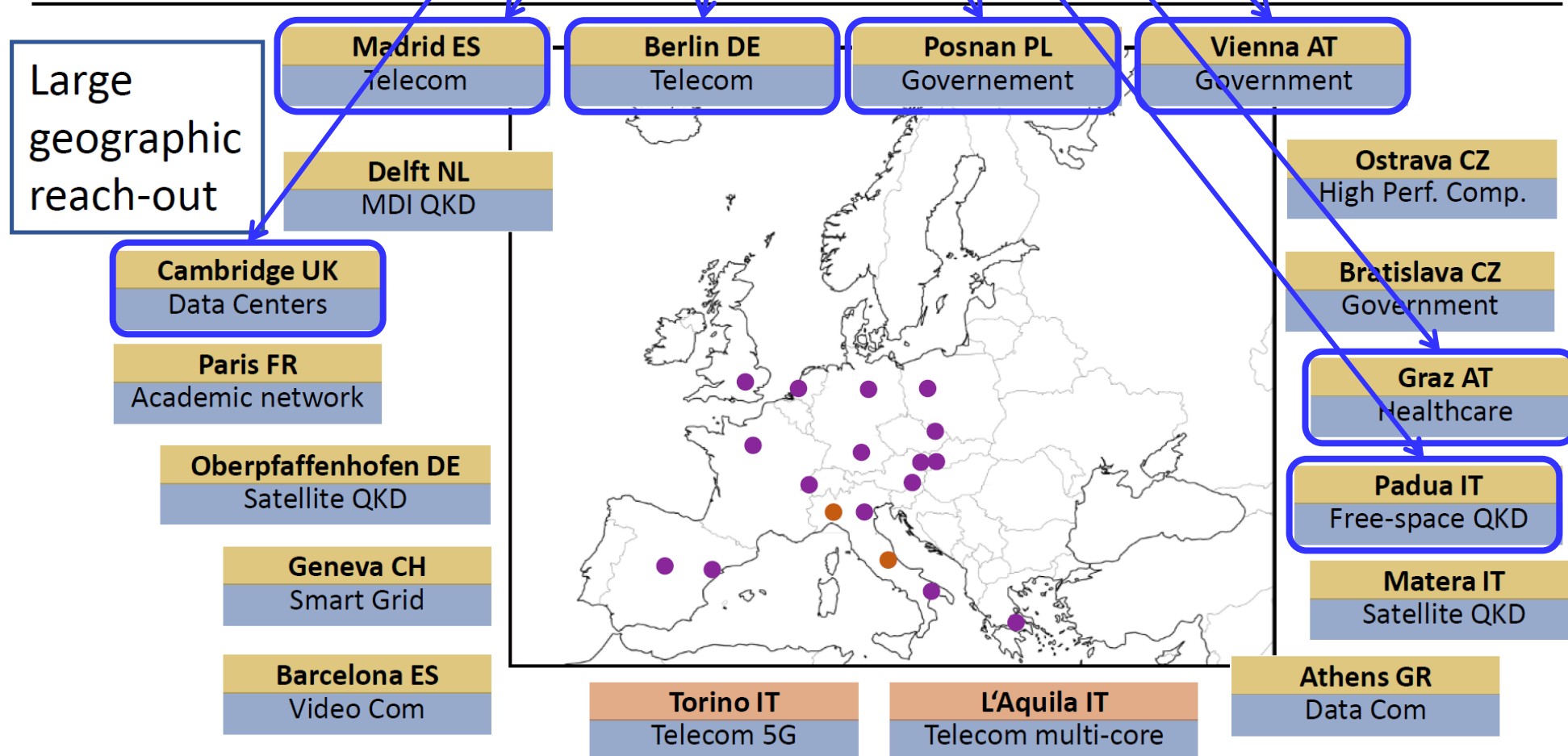
	東芝	スイスIDQ社	中国QCT社	中国Qasky社
装置外観		 <a href="https://www.idquantique.com/quantum-safe-security/products/cerberis3-qkd-system/">https://www.idquantique.com/quantum-safe-security/products/cerberis3-qkd-system/</a>	 <a href="http://www.quantum-info.com/English/product/quantum/2017/1013/407.html">http://www.quantum-info.com/English/product/quantum/2017/1013/407.html</a>	 <a href="http://www.qasky.com/en/display.asp?id=781">http://www.qasky.com/en/display.asp?id=781</a>
鍵生成速度	<b>毎秒300キロビット @50km</b>	毎秒6キロビット @60km	毎秒15キロビット @50km	毎秒40キロビット @50km
最大距離(損失)	<b>120km (24dB)</b>	75km (18dB)	85km	~ 100km
実績	海外10拠点の 実証フィールドで稼働中	10年以上の市場実績	中国国内で大規模な社会実装	

# 東芝の装置が欧州プロジェクト(Open QKD)の7つの拠点で稼働中

北米、シンガポール、韓国の拠点でも稼働

## 18 OpenQKD Testbed Sites

OPEN  QKD



# 2021年から量子ICTは新たなフェーズに（第5期中長期計画）

2021年、NICTが**量子セキュリティ拠点**に指定。**量子ICT協創センター**が発足。

量子セキュリティ・協創棟（2022年3月竣工）



量子ICTの研究  
開発と社会実装

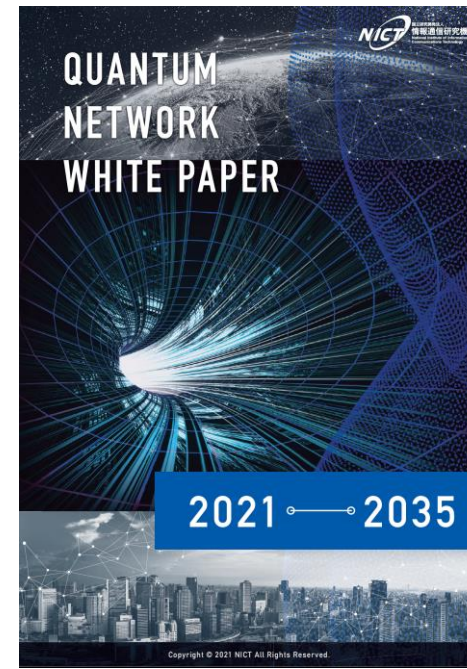
未来ICT研究所 量子ICT研究室（2001年～）



3号館

## 量子ネットワークホワイトペーパーを公開

- ・量子通信・量子暗号に関する最新動向
- ・量子ネットワークが実現する社会像・ユースケース
- ・その実現に向けてNICTが取り組む研究開発、ロードマップ、推進戦略など



# 量子セキュリティ拠点 (NICT、2021年2月～)

## 量子技術が拓く新たな情報セキュリティを社会へ届ける

1. 新たな融合領域『量子セキュリティ分野』を創成し、社会実装に取り組む。
2. 様々な量子技術の融合を図り、情報通信インフラに導入・統合し、『量子技術プラットフォーム』を構築する。

エコシステム構築に向けPOC



ベンダ：東芝、NEC  
キャリア：NS社、NC社、NA社、K社、SJ社  
クラウド事業者：SI社  
暗号ベンダ：I社  
カード事業者：T社  
部品メーカー：M社、Y社  
商社：M社  
金融機関：N社、M社、M社、S社、D社  
政府系機関：2機関

### 量子セキュリティ分野

### 量子コンピュータ分野

### 量子計測・センシング分野

### 量子技術プラットフォーム

高度な計算処理、計測・センシング、通信・暗号の機能を提供する新たな基盤

# 推進戦略

産学官の協創環境を整備しながら、研究開発、テストベッドでの実装・試験、社会展開、人材育成まで一気通貫で取り組む。



量子セキュリティ・協創棟 (NICT)  
2022年3月竣工

## 人材育成

- NICT Quantum Camp
- ・産学官連携による実践的なプログラム
- ・総合力のある量子ネイティブの育成

## 研究開発

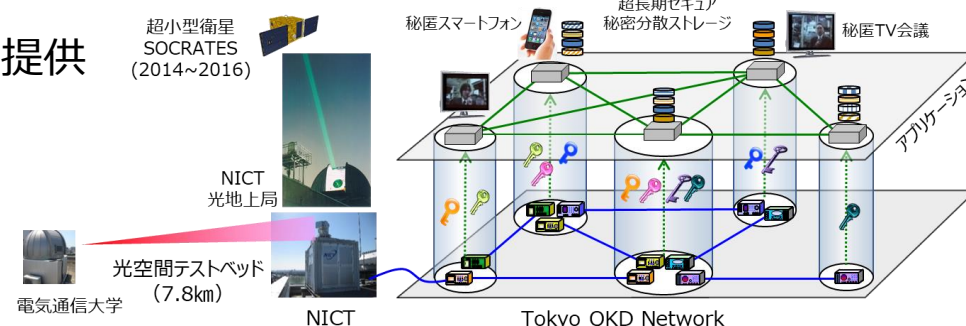
- 量子ノード 光量子制御、量子中継、量子計測標準
- 量子セキュリティ 量子暗号、現代暗号、ネットワーク技術、情報理論等との融合
- 衛星量子通信 量子技術の衛星搭載化
- 量子ネットワーク 地上網・衛星網の統合、グローバルネットワーク化

## 社会展開

- 標準化
- 知財
- 評価・認証制度
- 国際連携

## オープンテストベッド

- 産学官協創環境の提供
- 成果の実装、試験、企業への技術移転



# ロードマップ

2023年頃

ベンダー、通信事業者による  
量子暗号サービスの提供



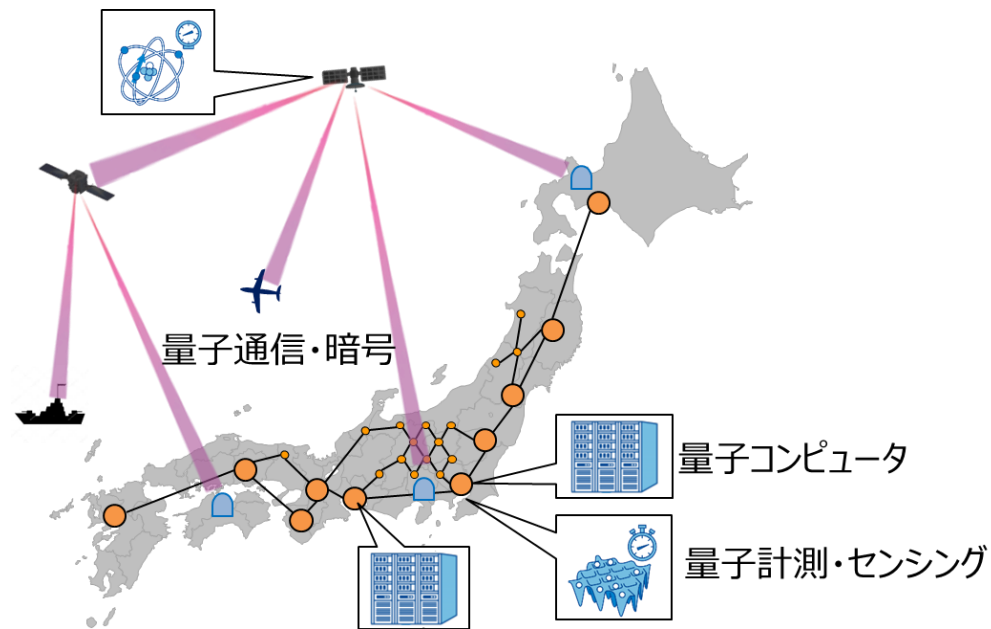
2025年頃

都市間の量子暗号通信網

- ・装置の量産化
- ・評価・認証制度の確立

2030年頃

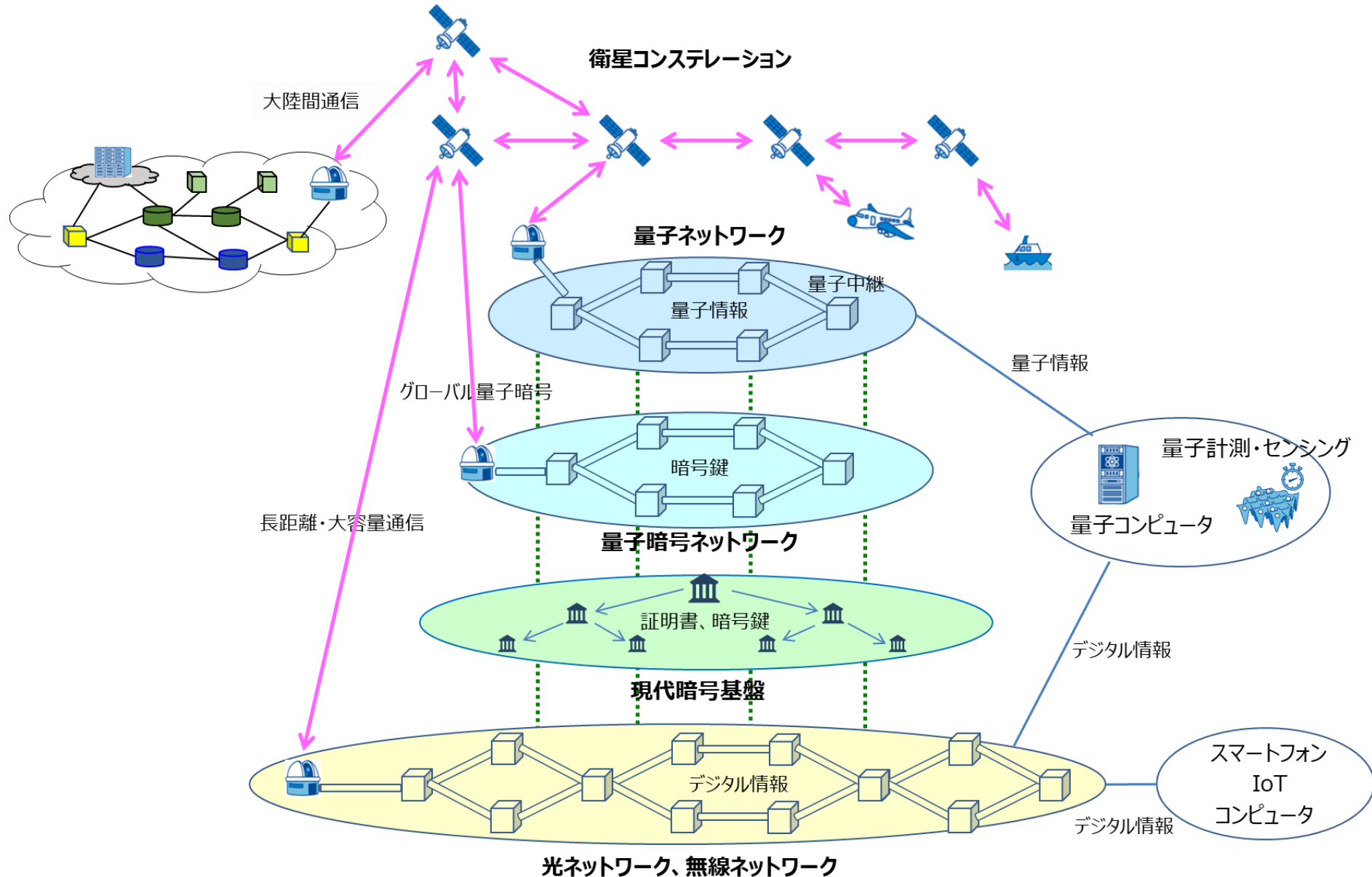
衛星・地上網の統合  
本格普及、ビジネスエコシステムの確立



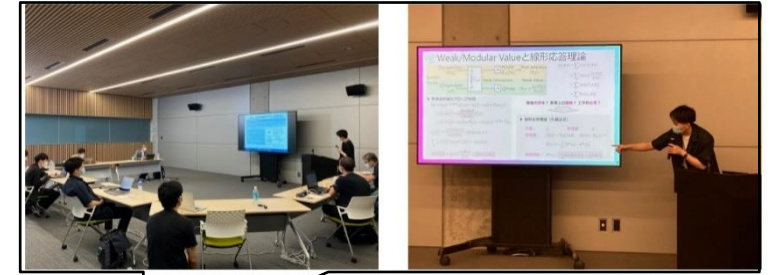
2035年頃

# 量子技術プラットフォーム

様々な量子技術の融合を図りグローバルネットワーク化



# 人材育成



## 若手チャレンジラボ (2022年度～)

NICTの研究アシスタントやインターン生として、  
先端的な研究開発に挑戦。  
産学官の協創環境の中で多様なメンバーと連携、交流。

## NICT Quantum Camp (2020年度～)

### 探索型プログラム

研究作業支援費を受給し講師らの指導の下、研究を実施。

### 体験型プログラム

高校生、高専生、大学生、大学院生、社会人。  
(講義) 量子セキュリティ、量子計算、量子計測標準  
(演習) 量子コンピュータ実機 (IBM Q) を利用  
(講師) 機構内外のトップ研究者17名

